TERMO DE REFERÊNCIA

1. DO OBJETO

Contratação de empresa especializada no fornecimento de equipamentos de informática, computadores, munitores, nobreak, projetor de multimídia, scanner de mesa, impressora, firewall, licença de software antivírus, licença pacote office business e tela de projeção para atender as necessidades internas da Federação da Agricultura e Pecuária do Estado de Rondônia - **FAPERON**, conforme especificações constantes no presente termo de referência.

2. JUSTIFICATIVA

A Federação da Agricultura e Pecuária do Estado de Rondônia – **FAPERON,** está em processo de reorganização e modernização operacional no desempenho de suas finalidades e atribuições em cumprimento das alíneas "e" e "f" do artigo 2º do Estatuto social desta entidade, tendo em vista a assinatura do Termo de Adesão e Compromisso assinado com a CNA do "Programa de Fortalecimento da Federação", que tem como objetivo criar e desenvolver o fortalecimento do sistema para o cumprimento da missão visando o atendimento do seu público com qualidade. Para isso necessitamos da readequação administrativa com aquisição de novos equipamentos de tecnologia que atenda as mudanças exigidas com o crescimento do agronegócio de Rondônia. Temos necessidade de implantar sistema de segurança das informações tecnológicas e de rede desta Federação e salvaguardar de forma segura todas as informações e dados de informação desta entidade. Ressaltamos ainda, que caso não seja realizado este investimento, há risco de comprometimento com o termo de compromisso CNA, pois já estamos já estamos em fase de contratação do corpo técnico que fara parte do programa.

Considerando a necessidade de comportar os novos funcionários técnicos, fornecendo estrutura física e tecnológica, dotada de condições necessárias para desenvolver as atividades laborais e a urgência da segurança das informações da federação.

Portanto, a aquisição se faz necessária para atender e acomodar os futuros funcionário, bem como a segurança das informações com tecnologia eficaz e segura, com intuito de proporcionar condições de trabalho e conforto.

3. ESPECIFICAÇÕES E QUANTIDADES DOS PRODUTOS

3.1 Os fornecedores contratados deverão entregar na sede da FAPERON dentro dos prazos estabelecidos os seguintes produtos conforme segue as especificações e quantidades abaixo:

Item	Descrição dos Equipamentos	UND	Qtd
01	Computador Desktop, com garantia *on-site*, pelo período de 36 (trinta e seis) meses, de acordo com as especificações técnicas constantes do Termo de Referência.	UND	15
02	Monitor LED entre 21,5" e 22,5" Widescreem com garantia *on-site*, pelo período de 36 (trinta e seis) meses de acordo com as especificações técnicas mínimas constantes no Termo de Referência	UND	20
03	Scanner de mesa com Alimentador Automático de Documento (ADF/AAD), com garantia *on-site*, pelo período de 36 (trinta e seis) meses de acordo com as especificações técnicas mínimas constantes no Termo de Referência.	UND	2
04	Servidor de aplicações e arquivos contendo Windows Server 2022 Standard , processador como no mínimo 17.000 pontos auferidos no site https://www.cpubenchmark.net/ , com suporte a segundo processador, 16 gb de memoria (Marcas de Referencia - DELL, LENOVO OU HP) 2TB de disco com suporte a sistema Raid, 0,1,5	UNI	01
05	Nobreak Senoidal de onda aproximada 700va	UND	15
06	Projetor de video (Data show) 3400 Lumens 3LCD (Marcas de Referencia - Epson, Benk, Optoma)	UND	02
07	Access Point coprporativo mimo 2x2 indoor (Marcas de referencia Aruba, Cisco, Ruckus, Cambium,	UND	02
08	Impressora multifuncional velocidade minima Impressão funções: Impressão, Cópia, Digitalização, (Marcas de referência HP, Kyocera, Lexmark)	UND	01
09	Firewall tipo apliance para rack 19" NG Camada 7 para pequena empresa (Marca de Referencia - Fortinet, Check Point, Sophos e Dell Sonic Wall)	UND	01
10	Licença de Software antivírus endpoint para estações e servidor pelo período de 3 anos	UND	25
11	Licença pacote office Business 2021 formato ESD PN: T5D-03487	UND	20
12	Impressora Multifuncional Jato de tinta contendo tanque externo	UND	06
13	Nobreak com potência mínima de 2200VA e 1300W	UND	01
14	Tela de projeção elétrica tensionada WideScreen 150 polegadas 3,32 m x 1,87	UND	01
15	Tela de projeção elétrica prime 1:1 WideScreen 110 polegadas 2,00 m x 2,00 m ttel-020	UND	01

Rua João Goulart nº 1843 – Bairro: Nossa Senhora das Graças – E-mail: faperon@faperon.br
Telefone: (69) 32148371 - Cep: 76804-126 – Porto Velho - Rondônia

16	Impressora Laser Colorida minimo 30 ppm	UND	01

1- COMPUTADOR DESKTOP CORPORATIVO

Especificações mínimas	Motivação
a) Todos os componentes visíveis integrantes do equipamento ofertado (gabinete, mouse e teclado) devem possuir mesma cor predominante; Ser do mesmo fabricante ou em regime de OEM e neste caso deverá ser comprovado através de documentação emitida pelo fabricante anexada à proposta, que atenderão às mesmas exigências de garantia, atendimento e prazo de solução, idênticos aos do equipamento principal CPU;	Facilitar a identificação dos componentes e a harmonia dos equipamentos; Garantir a procedência que mantém o mesmo padrão de garantia do fabricante para todos os componentes do equipamento.
b) Gabinete: Deverá ser do tipo Small Form Factor (SFF), de mesa, com dimensões aproximadas de 339mm W X 382mm D X 101mm H (LxPxA), contanto que não ultrapasse volumetria máxima de 13.100.000cm³; Possuir mecanismo de abertura que facilite a manutenção, instalação ou remoção de dispositivos (como HD, placas PCI, memória), podendo ser aberto e fechado sem uso de ferramentas (toolless); E possuir Sensor de Intrusão de Gabinete, conectado a placa mãe, ativo e configurado que crie alertas específicos para esse fim, visualizados por meio do software de gerenciamento; Não será aceito parafusos recartilhados, nem outra	Importante para adaptação em mobílias com tamanhos reduzidos. Essa modelagem/tecnologia garante a otimização da arquitetura das peças e do gabinete, bem como permitir a segurança contra intrusão do gabinete do equipamento, emitindo alertas e ainda a manutenção física do equipamento sem necessidade de usar ferramentas; Facilitar a operacionalização do equipamento e a visualização do status de funcionamento.

Rua João Goulart nº 1843 – Bairro: Nossa Senhora das Graças – E-mail: faperon@faperon.br
Telefone: (69) 32148371 - Cep: 76804-126 – Porto Velho - Rondônia

adaptação para atender a característica toolless; Botão liga/desliga e indicadores de atividade da unidade de disco rígido e do computador ligado (power-on) na parte frontal; Deverá ser fornecido auto falante interno ao gabinete capaz de reproduzir os sons gerados pelo sistema. O mesmo deverá estar conectado diretamente a placa mãe, sem uso de adaptadores;	
c) Interfaces: 06 (seis) interfaces USB nativas, sendo 02 (duas) portas frontais e 04 (quatro) portas traseiras (pelo menos 02 (duas) portas deverão ser do tipo USB 3.0, não sendo permitido o uso de adaptadores); 01 (uma) porta serial; 01 (uma) porta RJ-45, 10/100/1000 (nativa na placa mãe), Áudio de alta definição.	O mínimo de seis portas USB possibilita a utilização de vários dispositivos simultaneamente (mouse, teclado, pen drives, câmera fotográfica, GPS, câmera de vídeo, dentre outros).
d) Placa de rede (10/100/1000): Deverá suportar os padrões WoL e ASF 2.0 ou SNMP v3; Deverá ser possível habilitar sistema de gerenciamento DASH 1.1 ou iAMT com a placa de rede on-board, **não serão aceitas** placas de rede off-board ou quaisquer customização com dispositivos USB, PCMCIA ou similares;	A interface de rede com as características implementadas através de gerenciamento remoto permite ao administrador de TI otimizar o tempo com tarefas de suporte remoto aos desktops.
e) Placa mãe: Deverá ser do mesmo fabricante do equipamento ofertado ou em regime OEM, não sendo aceitas placas mãe de livre comercialização no mercado; Deverá possuir suporte para processadores de quatro	Os dispositivos do mesmo fabricante ou em regime de OEM garantem a procedência, qualidade e compatibilidade.

Rua João Goulart nº 1843 – Bairro: Nossa Senhora das Graças – E-mail: faperon@faperon.br
Telefone: (69) 32148371 - Cep: 76804-126 – Porto Velho - Rondônia

núcleos ou tecnologia semelhante;	
f) Processador: Arquitetura 64bits, com no mínimo 06 (seis) núcleos reais ou superior. Frequência mínima de 2.5 Ghz ou superior; Suporte a virtualização; Memória cache total de, no mínimo 18MB (dezoito megabytes); Deverá suportar processamento em 64 bits (modo AMD64 ou EM64T); Deverá ser projetado para efetuar computação simultânea de 32 bits e 64 bits; O cooler do processador deverá ser fabricado pelo fornecedor do processador ou fabricante do Equipamento ou fornecido em regime comprovado de OEM; Processador em linha de produção (Processadores descontinuados não serão aceitos).	Os processadores atuais possuem classificação de desempenho considerando a quantidade de núcleos que possuem. Os processadores com 4 núcleos são aplicados a atividades básicas sem necessidade de muita performance (exemplo edição de textos, navegação na internet); Processadores de 6 núcleos, são aplicados na execução de aplicativos que necessitem de mais recursos de processamento – como a execução de programas mais exigentes e utilização simultânea de vários aplicativos e janelas de navegação, como é o caso da rotina de trabalho de quase todos os setores do FAPERON. Além disso, todas as recentes aquisições de computadores obedeceram a esse padrão mínimo.
g) BIOS**:** Deverá ser desenvolvida pelo mesmo fabricante do microcomputador ou em regime de OEM; Deverá possuir chip de segurança TPM 1.2 nativo; Deverá suportar tecnologias de integração à rede como PXE, configuração e controle remotos; A interface de configuração deverá ser em, pelo menos, um dos idiomas: Português do Brasil ou Inglês; Deverá ser implementada em memória “flash”, atualizável diretamente pelo microcomputador; Deverá possuir a opção de salvar todos os parâmetros em um arquivo,	Os dispositivos do mesmo fabricante ou em regime de OEM garantem a procedência, qualidade e compatibilidade; Chip TPM é uma sigla que em inglês significa Trusted Platform

Rua João Goulart nº 1843 – Bairro: Nossa Senhora das Graças – E-mail: faperon@faperon.br
Telefone: (69) 32148371 - Cep: 76804-126 – Porto Velho - Rondônia

que poderá ser carregado em todos os equipamentos do mesmo lote, facilitando assim a replicação das políticas de segurança e dispositivos; Deverá possuir campo com número de série do equipamento devendo o mesmo poder ser lido remotamente via comandos SMBIOS; Deverá possuir campo editável, com recurso para registro de informações como, por exemplo, o número do patrimônio do equipamento devendo o mesmo poder ser lido remotamente via comandos SMBIOS;	Module – ou ainda – Módulo de Plataforma Segura, e vem embarcado na placa mãe dos computadores e tem a função de criptografar o conteúdo informado pelos usuários.
h) Chipset: Deverá suportar a expansão de memória para, no mínimo, 32 GB (trinta e dois gigabytes), padrão DDR4 de 2400 MHz, ou superior; Deverá suportar o barramento PCI Express x16; Deverá ser projetado para computação com uso eficiente da energia; Deverá suportar o padrão SMART IV ou superior; Deverá suportar a utilização de, no mínimo, 02 (dois) monitores independentes sem a necessidade de auxílio de uma placa de vídeo off-board;	Permite garantia de expansão de recursos tecnológicos dos equipamentos, para melhor desempenho e performance em novas demandas por recursos.
i) Memória RAM: Compatível com DDR4, velocidade de 2400 Mhz ou superior, com no mínimo 08 (oito) GB; Expansível a pelo menos 32 (trinta e dois) GB, distribuídos da seguinte forma:	A velocidade de operação da memória RAM está diretamente relacionada ao desempenho geral da máquina. Considerando a tecnologia DDR4 para memórias, busca-se maior economia energética, e ainda velocidade mínima de 2400Mhz permite taxa de transferência de até 12.800 MB/s, possibilitando

6

• (2x4GB) instaladas em dois módulos com 4GB cada, devendo estar vazios dois outros módulos, **ou** • (1x8GB) instalada em 1 módulo, devendo estar vazios três outros módulos.	excelente desempenho ao equipamento, avaliando o seu trabalho em conjunto com as especificações dos itens (e), e, (h). Além disso, essa configuração está projetada para o atendimento às necessidades do FAPERON pelos próximos cinco anos, no mínimo, permitindo sua expansão se necessário.
j) Disco Rígido: Uma unidade de disco rígido instalada (SSD/ NVMe, de no mínimo 256 GB de armazenamento, mínimo - Leitura/Gravação: 2100/1700 MB/seg ou superior;	Observando as características de bom desempenho operacional do equipamento, o disco rígido deve possuir requisitos técnicos que não prejudiquem o seu trabalho em conjunto com os itens (e), e, (h). A leitura das informações em um disco rígido está associada à velocidade de rotação do equipamento, quanto maior, melhor o desempenho obtido. Leitura/Gravação: 2100/1700 MB/seg ou superior; considera o padrão atual oferecido em discos rígidos sem prejudicar a performance do equipamento. A A capacidade mínima de armazenamento exigida de 256 GB considera o uso para o sistema operacional e a utilização do equipamento nas atividades cotidianas de auditoria e outras afins da FAPERON.
k) Conexões de Vídeo: Mínimo de 01 (uma) conexões de vídeo VGA e 01 (uma) DisplayPort ou 01 (uma) DVI, possibilitando a utilização simultânea de no mínimo 2 (dois) monitores;	O equipamento deve permitir a utilização de área de trabalho estendida, ou seja, utilização de até dois monitores funcionando como uma única área de trabalho. A implantação de sistema de informação de processo virtual faz com que haja necessidade de utilização simultânea de mais de um monitor de vídeo por máquina, possibilitando ganho de produtividade.

Rua João Goulart nº 1843 – Bairro: Nossa Senhora das Graças – E-mail: faperon@faperon.br
Telefone: (69) 32148371 - Cep: 76804-126 – Porto Velho - Rondônia

l) Teclado: Padrão ABNT2, com ajuste de inclinação, com conector USB, sendo vedado o uso de adaptadores;	O padrão ABNT2 é o padrão utilizado pela FAPERON. Conector tipo USB, sem adaptador, é pela função hot swap, ou seja, que possibilita retirar e/ou colocar o periférico em funcionamento, sem a necessidade da reinicialização do equipamento.
m) Mouse: Apontador (mouse) com tecnologia óptica e resolução mínima de 1000 dpi (sem esfera) de 2 (dois) botões e 1 (um) botão de rolagem (“scroll”), com conector USB, sendo vedado o uso de adaptadores;	A opção pelo mouse óptico é pelo fato de não possuírem partes móveis, sendo assim, a durabilidade aumenta e o acúmulo de sujeira diminui. Conector do tipo USB é justificado pelo mesmo motivo apontado no item (l). A tecnologia laser possui maior acurácia na definição do dispositivo o que evita correções de posicionamento consequentemente aumentando a produtividade;
n) Todos os computadores deverão ser entregues com o seguinte sistema operacional já instalado: Microsoft Windows 11 Professional ou Enterprise, 64 bits, português (Brasil), devidamente licenciado - com licença definitiva em nome da– FAPERON. Deverão constar da Lista de compatibilidade Microsoft Windows Catalog para o sistema operacional Windows 11 ou superior. Também deverão ser compatíveis com Linux;	A versão mais atual de sistema operacional utilizada pelos maiores fabricantes de TI é o Windows 11, que também é a versão que será utilizada em 100% do parque de desktops e notebooks do FAPERON; Esse sistema possui muitas versões, sendo a Professional ou Enterprise uma das mais completas; A arquitetura de 64 bits, possibilita a utilização plena dos recursos dos processadores disponíveis no mercado atualmente, e também, com esta arquitetura uma versão mais completa do Windows 11 consegue trabalhar com até 192 Giga Bytes de memória RAM, superando a limitação de 4 GB da arquitetura tradicional de 32 bits.
o) Documentação e Help (ajuda) on-line;	Utilizada pela equipe técnica de apoio ao usuário.
p) O equipamento deverá oferecer os recursos: ▪ Wake on Lan, que permite ligar o microcomputador	Possibilitar atuação remota com maior agilidade na administração, atualização, gerenciamento do sistema e suporte dos recursos tecnológicos. Garantir a identificação, integridade e segurança

8

utilizando o recurso de ativação da máquina via LAN; ▪ Alterar remotamente a BIOS, possibilitando fazer atualização da BIOS e drivers do equipamento ofertado (habilitar/desabilitar senha, portas USB, etc); ▪ Reinicializar o microcomputador remotamente; ▪ Identificar os componentes do microcomputador e suas características, coletando no mínimo as seguintes informações: tipo do processador, quantidade de memória, tamanho do HD, número de série do equipamento, número do ativo fixo e tipo do sistema operacional; ▪ Alterar remotamente arquivos de configuração do sistema; ▪ Permitir ao administrador de TI interagir com a interface gráfica de usuário mesmo que o sistema operacional esteja inoperante ou mesmo sem a presença de um sistema operacional; ▪ Detectar e alertar intrusão de gabinete; ▪ Possuir dispositivo de tranca do gabinete	(física e lógica) dos dispositivos e dos dados armazenados no equipamento.

Rua João Goulart nº 1843 – Bairro: Nossa Senhora das Graças – E-mail: faperon@faperon.br
Telefone: (69) 32148371 - Cep: 76804-126 – Porto Velho - Rondônia

através de cadeado em aço inoxidável com chave tipo canhão micromecânica anti-clonagem com segredo único (em substituição ao cadeado, será aceita fechadura eletrônica interna ao gabinete gerenciada pela BIOS); ▪ Possuir slot do tipo Kensington para sistema de travamento e ancoragem do conjunto CPU, monitor e cabos dos periféricos; ▪ O fabricante deverá disponibilizar software capaz de verificar automaticamente novas atualizações ou ainda possuir um sistema de alerta via e-mail sobre disponibilidade de novas atualizações; ▪ Todas as especificações deste item devem ser comprovadas através de catálogos, folders, manuais do equipamento ou declaração fornecida pelo próprio fabricante;	10

q) Compatibilidades e Certificações:

1. Deve ter compatibilidade com o padrão DMI (Desktop Manager Interface) ou mais recente DMTF (Desktop Management Task Force), comprovado através de documentação expedida pelo fabricante, indicando que os equipamentos estão dentro dos requisitos de gerenciamento remoto da DMTF;

▪ TCU - Acórdão nº 7549/2010.

2. Deverá possuir, integrado à placa-mãe do computador (on-board), sem adaptações, subsistema de segurança TPM (trusted platform module) compatível com a norma TPM Specification Version 1.2 ou superior especificada pelo TCG (Trusted Computing Group);

- Padrão de segurança.

3. O equipamento deve ser compatível com Energy Star 5.0 ou superior (apresenta um consumo de energia mais baixo e ao mesmo tempo, protege o meio ambiente utilizando produtos e práticas específicas). A certificação será comprovada através do fabricante do equipamento ou da página http://www.energystar.gov, sendo necessário identificar a marca e o modelo ou família do equipamento. Poderão ser fornecidos atestados ou certidões que comprovem que o equipamento é compatível com Energy Star, emitido por instituto credenciado junto ao INMETRO, ou por instituição pública oficial;

- TCU - Acórdão nº 670/2013.

4. Possuir fonte de alimentação tipo ATX ou BTX para corrente alternada com tensões de entrada de 100 a 240 VAC (+/-10%), 50-60Hz, com ajuste automático, suficiente para suportar todos os dispositivos internos na configuração máxima admitida pelo equipamento (placa principal, interfaces, discos, memórias e demais periféricos) e que implemente PFC (Power Factor Correction) ativo com eficiência igual ou superior a 89% a 100% de carga (PFC 80+). O modelo de fonte fornecido deve estar cadastrado no site www.80plus.com na categoria Platinum ou superior (determina os valores de eficiência energética mínima). Poderão ser fornecidos atestados ou certidões emitidas por instituto credenciado junto ao INMETRO, ou por instituição pública oficial, que comprovem que o equipamento é aderente ao padrão de eficiência energética exigido;

- TCU - Acórdão nº 1147/2014.

5. O equipamento deve estar de acordo com a diretiva RoHS, (Restriction of Hazardous Substances) que proíbe que certas substâncias nocivas sejam usadas em processos de fabricação de produtos eletro eletrônicos (cádmio (Cd), mercúrio (Hg), cromo hexavalente (Cr(Vl)), bifenilos polibromados (PBBs), éteres difenil-polibromados (PBDEs) e chumbo (Pb)), sendo fornecida certificação emitida por instituto credenciado junto ao INMETRO, por instituição pública oficial, ou ainda,

a comprovação deste requisito por intermédio da certificação EPEAT, desde que apresente explicitamente tal informação;

- TCU - Acórdão nº 1147/2014.

6. Deve ter compatibilidade com EPEAT (Eletronic Product Environmental Assessment Tool), da agência de proteção ambiental (EPA), com certificado na categoria GOLD (que são requisitos do EPEAT para especificações de hardware, processos de adequação ecológica, toda cadeia de logística reversa da empresa, que incluem dentre outros, a coleta de produtos obsoletos e embalagens) comprovada através de atestados ou certidões que comprovem explicitamente que o equipamento é aderente ao padrão de eficiência energética EPEAT, emitido por instituto credenciado junto ao INMETRO, ou por instituição pública oficial. Será admitida como comprovação também, a indicação que o equipamento consta no site www.epeat.net categoria GOLD;

- TCU - Acórdão nº 1147/2014.

7. O equipamento deverá possuir certificação de compatibilidade com a norma IEC-60950 (que estabelece padrões que visam reduzir ao mínimo o risco de incêndio, choque elétrico ou outro tipo de dano ao usuário que entrar em contato com o equipamento) ou similar emitida por instituição acreditada pelo INMETRO, ou ainda, por instituição pública oficial;

- TCU- Acórdão nº 1147/2014.

8. Todos os cabos e conectores de conexão à rede elétrica deverão seguir o padrão NBR-14136;

- Norma brasileira que estabelece padrões para plugues e tomadas.

9. O equipamento deverá apresentar compatibilidade eletromagnética e de radiofrequência IEC-61000, CISPR22, CISPR24 (que definem os métodos de teste, os limites de interferência eletromagnética que o equipamento pode emitir, e, limites relacionados a surtos ou transientes (instabilidades) que o equipamento deve suportar) comprovado através de certificado ou relatório de avaliação de conformidade emitido por órgão credenciado pelo INMETRO, ou por instituição pública oficial. São certificações que focam na segurança operacional do equipamento e na sustentabilidade ambiental;

- TCU - Acórdão nº 2.403/2012.

10. Deve possuir certificado NBR-10152, ou ISO-7779, ou ISO 9296, ou equivalente (normas que tratam de padrões para emissão de ruídos acústicos);

- TCU - Acórdão nº 1147/2014.

11. Deve possuir certificado ISO-14001 válidas, ou similar, emitido por instituto credenciado junto ao INMETRO, ou por instituição pública oficial (foca a proteção ao meio ambiente e a prevenção da poluição, equilibrando-a com as necessidades sócio econômicas do mundo atual);

- TCU - Acórdão 2.403/2012.

12. Deve possuir compatibilidade com sistemas operacionais Microsoft Windows 11 Professional ou Enterprise (64 bits). O modelo do equipamento deve constar da lista de Hardware Compatível da Microsoft – Microsoft Windows Catalog (HCL) (que compreende uma série de testes de hardware e software que asseguram a compatibilidade do equipamento com o produto Microsoft Windows). A comprovação de compatibilidade será efetuada pela apresentação do documento Hardware Compatibility Test Report emitido especificamente para o modelo no sistema operacional ofertado. Sitio: https://sysdev.microsoft.com/en-US/Hardware/LPL/, ou outro link que o substituir.

- TCU - Acórdão nº 1147/2014.

13. Todos os certificados como: Energy Star, EPEAT, HCL, NBR 10152, ISO 7779, ISO 9001, ISO 14001, IEC 60950, IEC 61000, CISPR22, CISPR24 e DMTF devem ser anexados junto à proposta durante o certame.

r) Todos os computadores e seus acessórios deverão ter garantia on-site de 36 (trinta e seis) meses prestada pelo FABRICANTE, conforme	Serviços de garantia para atualização e substituição de componentes de hardware e acessórios dos computadores corporativos do FAPERON

Rua João Goulart nº 1843 – Bairro: Nossa Senhora das Graças – E-mail: faperon@faperon.br
Telefone: (69) 32148371 - Cep: 76804-126 – Porto Velho - Rondônia

condições definidas neste termo.	
s) Garantia do fabricante	3 (três) anos On Site

2- DETALHAMENTO DAS ESPECIFICAÇÕES TÉCNICAS MÍNIMAS DO ITEM MONITOR 21,5 a 22,5”

ESPECIFICAÇÕES	DETALHAMENTO
Tela	• Entre 21,5” e 22,5” de LED widescreen, base com ajuste de altura, inclinável e com giro de tela de 90º (Pivot Rotation) sem adaptações externas.
Ângulo de visão	• Mínimo de 170° horizontal e 160° vertical.
Resolução	• Mínima de 1600 x 900 pixels. • Deve ser Antirreflexivo e Antiestático.
Tempo de Resposta	• Mínimo de 5ms.
Suporte de Cores	• Mínima de 16 Milhões
Contraste	• Mínimo de 5.000.000:1.
Cabos	• Deverá acompanhar cabos VGA e DVI-D.
Cor	• Deverá predominar a cor preta.
Conectividade	• 1 DP (versão 1.2) • 1 HDMI (versão 1.4) • 1 VGA • 1 porta USB 3.0 para upstream • 2 portas USB 3.0 laterais
Base	• Deverá acompanhar base com ajuste de altura, inclinável e com giro de tela de 90º (Pivot Rotation) sem adaptações externas.
Energia	• Fonte de alimentação com ajuste automático de voltagem, suportando as faixas de tensão de 100-240VAC.
Certificação	• Certificado ENERGY STAR
Software e utilitários	• Drivers e softwares deverão estar inclusos

Rua João Goulart nº 1843 – Bairro: Nossa Senhora das Graças – E-mail: faperon@faperon.br
Telefone: (69) 32148371 - Cep: 76804-126 – Porto Velho - Rondônia

Garantia do fabricante:	• 3 (três) anos de garantia On Site
	•

3- DETALHAMENTO DAS ESPECIFICAÇÕES TÉCNICAS MÍNIMAS DO ITEM (SCANNER COM ADD – MESA)

Especificações mínimas

Resolução de saída: 600 dpi (mínimo)
Modo de digitalização: Simplex (frente) e Duplex (frente e verso) através do alimentador automático (ADF/AAD);
Capacidade do Alimentador (ADF/AAD): 50 folhas (mínimo)

Velocidade Mínima:
Simplex: 40 ppm (em 300 dpi)
Simplex: 60 ppm (em 200 dpi)
Duplex: 80 ipm (em 300 dpi)
Duplex: 120 ipm (em 200 dpi)
Conectividade: USB 2.0 (mínimo)
Ciclo de Trabalho: 4.000 folhas / dia (mínimo)

Tamanho de documento: Permitir até tamanho A4 (210 mm x 297mm) (mínimo)
Gramatura do papel: Permitir papel com gramatura entre 41 a 210g/ m²
Alimentação de energia: Bivolt 110/220v
Outros: Deve vir acompanhar o de software OCR que grave nos seguintes formatos ODT, DOC e PDF

Sistemas Operacionais Compatíveis: Certificado para Windows Vista®, Microsoft®, Windows®, 8.1, Windows 11, Windows Server 2012, 2019, Linux e Mac

Garantia do fabricante: 1 (um) ano

4- DETALHAEMNTO DAS ESPECIFICAÇÃÕES TÉCNICAS MÍNIMAS DO ITEM (SERVIDOR DE APLICAÇÕES)

Processador Intel® Xeon® E-2336 ou equivalente com no mínimo 17.000 pontos no site https://www.cpubenchmark.net/cpu_list.php
• 2x 8GB, 3200MHz
• 2x DISCOS 2TB 2,5” 7.200 RPM SATA RI Hot-plug
• Sistema Operacional opcional Windows Server® 2022 Standard, 16 núcleos, instalação de fábrica, sem CALs, vários idiomas
• 3 anos de assistência local on site

- 16GB DDR4 3200MHz (2X8GB, ECC, UDIMM, BCC)
- 2X DISCO 2TB 7200 RPM 2.5" Hot Plug AG Drive, 3.5" HYB CARR, 1 DWPD
- C3, RAID 1 para 2 HDDs ou SSDs (tipo/velocidade/capacidade correspondente)
- Chassi de 3.5" para até 8 Hot Plug discos rígidos e AIC PERC, hot-plug PSU
- **Compartimentos frontais**
  Até 4 SAS/SATA (disco rígido/SSD) de 3,5 pol., min. de 64 TB
  Até 8 SAS/SATA (disco rígido/SSD) de 3,5 pol., min. de 128 TB
  deverá suportar unidades de 2,5 polegadas em porta-discos híbridos de 3,5 polegadas)
- **Controladores internos**
  PERC H755, PERC H345 e HBA355i ou equivalente

  Controladores externos
  HBA355e ou Equivalente

  RAID de software
  S150 ou equivalente

  Inicialização interna
  Boot Optimized Storage Subsystem (BOSS-S2): 2 SSDs M.2 de 240 GB ou 480 GB com HWRAID para hardware
  Módulo com duas placas SD internas ou USB interno
- Firmware autenticado por criptografia
  Inicialização segura
  Exclusão segura
  Raiz de confiança do silício
  Bloqueio do sistema (exige o iDRAC9 Enterprise ou Datacenter)
  TPM 1.2/2.0 FIPS, certificação CC-TCG, China NationZ para TPM 2.0
- **Integrado/no servidor**
  iDRAC9
  iDRAC Service Module

Rua João Goulart nº 1843 – Bairro: Nossa Senhora das Graças – E-mail: faperon@faperon.br
Telefone: (69) 32148371 - Cep: 76804-126 – Porto Velho - Rondônia

iDRAC Direct

Consoles
OpenManage Enterprise
Plug-in do OpenManage Power Manager
Plug-in do OpenManage SupportAssist
Plug-in do OpenManage Update Manager

Mobilidade
OpenManage Mobile

Ferramentas
API RESTful do iDRAC com Redfish
Interface de linha de comando da RACADM
IPMI
Utilitário de atualização do sistema
Atualizar catálogos

OpenManage Integrations
BMC® Truesight
Microsoft® System Center
Módulos RedHat® Ansible®
VMware® vCenter e vRealize Operations Manager

OpenManage Connections
IBM Tivoli® Netcool/OMNIbus
IBM Tivoli® Network Manager IP Edition
Micro Focus® Operations Manager
Nagios® Core
Nagios® XI

- Bronze (a cabo) de 450 W CA/100-240 V
  Platina de 600 W CA/100-240 V
  600 W CC/240 V
- **Opções de rede**
  2 LOMs de 1 GbE

Portas frontais
1 porta iDRAC Direct (USB Micro-AB)
1 USB 3.0

Portas traseiras
5 USB 2.0
1 USB 3.0
1 porta serial
1 iDRAC
1 VGA

Portas internas
1 USB 3.0 (opcional)

- **PCIe**
  2 slots PCIe de 4ª geração, 1 slot PCIe de 3ª geração

  Placa de vídeo
  1 VGA
- Tampa de segurança opcional
- **Altura maxima**
  400,00 mm

  Largura
  200 mm
  Profundidade
  600,00 mm já incluso a tampa frontal

  Peso máximo
  36,00 kg

  Garantia de: 5 (Cinco) Anos on site

5- DETALHAMENTO DAS ESPECIFICAÇÕES TÉCNICAS MÍNIMAS DO ITEM (NOBREAKS DE ONDA SENOIDAL APROXIMADO 700VA)

Cor predominante: Preto
Tensão de entrada: 115V - 220V Bivolt
Tensão de saída: 115V Padrão Brasileiro de Plugues e Tomadas (Plugue NBR 14136 10A/250V - pino de 4mm de diâmetro
Potência: 700 VA / 490 W ou superior
Fator de potência: 0,5 ou superior
Forma de onda do inversor: Senoidal aproximada
Número de tomadas: mínimo 4 (quatro) tomadas Padrão Brasileiro de Plugues e Tomadas (Plugue NBR 14136 10A/250V - pino de 4mm de diâmetro)
Estabilizador: mínimo de 3(três) estágios
Bateria interna: 1x bateria 12 V

Autoteste de inicialização: para ao ser ligado, o nobreak testa os circuitos internos;
Leds coloridos no painel frontal para indicam as condições de funcionamento do nobreak - modo rede, modo inversor/bateria, final de autonomia, subtensão, sobretensão.
Alarme audiovisual: alarme para sinalização de eventos como queda de rede, subtensão e sobretensão, fim do tempo de autonomia e final de vida útil da bateria

Garantia 1 (um) ano

6- DETALHAMENTO DO ITEM (Projetor de vídeo) (Data show)3400 Lumens 3LCD (Marcas de Referência - Epson, Benk, Optoma)

>Sistema de projeção
- Tecnologia Epson 3LCD de 3 chips
- Método de projeção: Frontal / Traseiro / instalado no teto

>Brilho
- Brilho em cores: 3.400 Lumens
- Brilho em branco: 3.400 Lumens

>Resolução
- Resolução nativa: XGA
- Relação de aspecto: 4:3
- Número de pixels: 768.432 pixels (1024 x 768) x 3

>Caracteristicas
- Método de projeção: Matriz ativa TFT de poli-silício
- Relação de contraste: Até 15.000:1
- Reprodução de cor: Até 1 bilhão de cores
- Split Screen: sim

>Visor LCD
- não informado

>Audio
- sim, 1x 5W
- Ruído do ventilador: 28 dB / 37 dB

>Lente de Projeção
- Tipo: Zoom Ótico (Manual) / Foco (Manual)
- Número - F: 1,49-1,72
- Relação de zoom: 1-1,2
- Distância focal: 16,9 mm-20,28 mm
- Tampa da lente: Slide lens shutter
- Correção Trapezoidal Keystone: Vertical (-30° +30º) e Horizontal (-30° +30º)

>Tamanho da tela
- 30" a 300" (0,89 m - 10,95 m)

>Conectividade
- Entrada do computador: 2x D-sub15
- 1x HDMI
- 1x USB tipo A (Memória USB imagens / Módulo Wireless / Atualização de Firmware)
- 1x USB tipo B (display USB, mouse, Atualização de Firmware)

- 1x Vídeo RCA
- 1x RS-232C
- Saída monitor: 1x
- Entrada áudio RCA: 2x RCA (1x Branco, 1x Vermelho)
- Entrada áudio stereo mini: 2x
- Saída áudio stereo mini: 1x
- LAN - RJ45: x1
- Wireless: OPCIONAL

>Lampada - Caracteristicas
- Tipo de lâmpada: 210W UHE
- Vida útil da lâmpada: 6.000 horas (Normal); 12.000 horas (Eco)

>Alimentação
- Voltagem da fonte de alimentação: 100 - 240 V AC +/- 10%, 50/60 Hz
- Consumo de energia: 100-120V: 326W (Normal) - 237W (Eco); 220-240V: 309W (Normal) - 227W (Eco)

>Gabinete
- Trava Kensington® Segurança barra de segurança
- Dimensões (L x P x A): 30,2 x 24,9 x 8,7 cm (sem os pés)
- Peso: 2,7 Kg

>O que há na caixa
- Projetor
- Controle remoto com 2 pilhas AA
- Cabo de energia (1,8 m)
- Cabo do computador VGA (1,8 m)
- Manual de instalação

7- DETALHAMENTO DAS ESPCIFICAÇÕES TÉCNICAS MINIMA DO ITEM (Access Point corporativo mimo 2x2 indoor) (Marcas de referência Aruba, Cisco, Ruckus, Cambium, Huawei)

ACCESS POINT CORPORATIVO 802.11AC MIMO 2X2

Access Point deve operar em ambientes interno (wireless indoor);

Possuir Antena Omnidirecional MIMO 2X2;

Possuir capacidade de cobertura de até 100 metros de raio;

Deverá atender aos padrões IEEE 802.11a, IEEE 802.11b, IEEE 802.11g,

IEEE 802.11n e IEEE 802.11ac com operação nas frequências 2.4 GHz e 5

GHz de forma simultânea;

Operar no range de frequência DUAL BAND, 2,4 GHz e 5 GHz;

Possuir kit de fixação

Possibilitar a configuração de até 16 SSID;

Possuir suporte ao padrão IEEE 802.11q (VLAN);

Possuir suporte ao protocolo DHCP (modo servidor);

Possuir o recurso de Proxy web com as seguintes funcionalidades;

Possibilitar filtro por domínio;

Possibilitar filtro por URLs;

Possibilitar filtro por expressão regular;

Possuir o recurso de Captive portal (hotspot);

Possibilitar a personalização da página de acesso;

Possibilitar a conexão de no mínimo 256 (Duzentos e cinquenta e seis) clientes simultâneos

Possibilitar o filtro de acesso baseado em usuário/senha e endereço MAC;

Possibilitar o filtro de camada 4 (Baseado no modelo de referencia OSI);

Possibilitar o filtro de camada 7 (Baseado no modelo de referencia OSI);

Possuir suporte aos padrões IEEE 802.11i;

Permitir a configuração de no mínimo 02 (dois) servidores RADIUS;

Operar em 110/220V.

Garantia mínima de 12 meses

8- DETALHAMENTO TECNICO MINIMO DO ITEM (Impressora multifuncional velocidade minima Impressão funções: Impressão, Cópia, Digitalização, (Marcas de referência HP, Kyocera, Lexmark)

CONECTIVIDADE Mínimo de: Uma Porta USB 2.0 de alta velocidade (dispositivo); porta de rede Fast Ethernet 10/100/1000 Base-TX integrada;); Sem fio Capacidade sem fio, Padrão (Wi-Fi 802.11b/g/n/5G).
Cópia
Configurações de copiadora
Número de cópias; Mais claro/Mais escuro; Otimizar; Papel; Cópia de múltiplas páginas; Modo Rascunho
Número mínimo de cópias 90 cópias
Configurações de redução/ampliação de cópia 25 a 400%
Velocidade de cópia (preto, normal) mínimo 40 cpm

Resolução da cópia: Mínimo de 600 x 600 dpi
Especificações de ambiente
Emissões de potência sonora máxima 7,0 B(A) (impressão a 40 ppm)
Faixa operacional de umidade 30 a 70% de umidade relativa
Umidade para armazenamento 10 a 90% de umidade relativa
Faixa de temperatura operacional recomendada (Celsius)
17,5 a 25 °C Faixa de temperatura operacional recomendada (Fahrenheit)
63,5 a 77 °F
Variação de temperatura para armazenamento (Celsius) -20 a 60 °C
Variação de temperatura para armazenamento (Fahrenheit) -4 a 140 °F
Memória e processador
Processador mínimo de 1.200mhz
Memória: mínimo 512 GB
Recursos de impressão móvel
Suporte a serviços de impressão móvel Apple AirPrint;; Google Cloud Print 2.0; Certificação Mopria; Wi-Fi Direct
REDE-Protocolos de rede minimo suportados: TCP/IP: IPv4; IPv6; Modo IP direto; LPD; SLP; Bonjour; Descoberta WS; BOOTP/ DHCP/ AutoIP; WINS; SNMP v 1/2/3; e HTTP/HTTPS Manuseio de papel
Capacidade de entrada da bandeja
Mínimo de 250 folhas
Capacidade de saída
Mínimo de 150 folhas
Tamanhos de mídia compatíveis
A4; A5; A6; B5 (JIS)
Tamanhos de mídia suportados
Carta; Ofício; Executivo; 8,5 x 13 pol; envelopes
Tamanhos de mídia, personalizados (sistema métrico)
76 x 127 a 216 x 356 mm
Tamanhos de mídia, personalizados
3 x 5 a 8,5 x 14 pol.
Tipos de mídia
Papel (laser, papel comum, foto, rígido, velino), envelopes, etiquetas, cartões, cartões postais
Peso de mídia suportado Mínimo de 60 a 163 g/m²
Peso de mídia suportado Mínimo de 16 a 43 lb
Manuseio de papel - ADF
Capacidade do alimentador automático de documentos
45 folhas
Tamanho da mídia (ADF)
A4; Carta; Ofício
Peso de mídia suportado ADF 70 a 90 g/m²
Peso de mídia suportado, ADF 18,5 a 24 lb
Dimensões físicas
Dimensões máximas (L x P x A)
423,1 x 511,4 x 423,7 mm
Dimensões máximas (L x P x A)

Rua João Goulart nº 1843 – Bairro: Nossa Senhora das Graças – E-mail: faperon@faperon.br
Telefone: (69) 32148371 - Cep: 76804-126 – Porto Velho - Rondônia

16,7 x 20,1 x 16,7 pol.
Peso máximo 8,0 kg
Peso 17,5 lb
Liga/desliga
Tecnologia para economia de energia
Tipo de fonte de alimentação Interior
Fonte de alimentação
110 volts tensão de entrada: 110 a 127 VAC (+/- 10%), 60 Hz/50 Hz, 4,8 A;
Consumo de energia
Maximo de 570 watts (impressão ativa), 5,0 watts (pronto), 1,0 watts (suspensão), 0,05 watts (Desligar/Acordar automaticamente USB, habilitado no envio), 0,05 watts (Auto-off/Manual-on), 0,05 (Manual Off)
Cartuchos de impressão
Quantidade de cartuchos de impressão 2 (dois_
1 (um) Preto inicial para no mínimo impressão de 3.000 paginas
1 (um) Preto de alto rendimento para no mínimo impressão de 10.000 paginas
Tecnologia de impressão
Laser
Impressão frente e verso automático
Resolução de impressão (melhor ajuste)
1200 x 1200 dpi,
Área de impressão (sistema métrico)
214 x 356 mm
Área de impressão (padrão dos EUA)
3 x 5 a 8,5 x 14 pol.
Ciclo de trabalho mensal
Mínimo de 70.000 páginas
Linguagens de impressão
PCLmS, URF, PWG
Recursos do software de impressora inteligente
ePrint, Apple AirPrint, Tecnologia Instant-on, cartuchos JetIntelligence
Digitalização
Tecnologia de digitalização
CIS
Velocidade de digitalização (normal)
Mínimo de 30 ppm
Resolução de digitalização, hardware
Minimo 1200 x 1200 6pi (colorido e mono, ADF), 1200 x 1200 dpi (colorido, scanner de mesa), até 1200 x 1200 dpi (mono, de mesa)
Níveis de escala de cinza
256
Profundidade de bits
24 bits
Tamanho da digitalização de mesa 215,9 x 297 mm
Tamanho de digitalização de mesa 8,5 x 11,7 pol.

Rua João Goulart nº 1843 – Bairro: Nossa Senhora das Graças – E-mail: faperon@faperon.br
Telefone: (69) 32148371 - Cep: 76804-126 – Porto Velho - Rondônia

Tamanho mínimo da digitalização ADF 148,5 x 210 mm
Tamanho mínimo de digitalização ADF 5,9 x 8,3 pol.
Tamanho máximo da digitalização ADF 215,9 x 297 mm
Tamanho máximo de digitalização ADF 8,5 x 11,7 pol.
Versão do Twain Versão 2.1 ou superior
Gerenciamento e segurança
Servidor Web integrado de rede protegido por senha; ativar/desativar portas de rede; Alteração de senha da comunidade SNMPv1
Painel de operação em tela de toque colorida de no mínimo 3” (polegadas)
Sistemas operacionais de rede compatíveis:
Windows 10, 8, 7 (32-bit ou 64-bit), Windows XP SP3 ,Apple OS X v10.11 , Linux
Garantia:1(um) ano de garantia

9- DETALHAMETO TÉCNICO MINIMO ÍTEM (Firewall tipo apliance para rack 19" NG Camada 7 para pequena e média empresa) (Marca de Referencia - Fortinet, Check Point, Sophos e Dell Sonic Wall)

FIREWALL Next Generation contemplando Suporte minimo de 3(três) Anos

Gerenciamento: Deverá ser gerenciável por interface gráfica WEB (GUI), com acesso seguro HTTPS (da rede interna ou remotamente) e também através de linha de comando SSH para procedimentos avançados, sem a necessidade de instalação de programa de gerência ou de terceiros.

Processamento (hardware): Deverá possuir no processamento, mínimo de 4 processadores de no minimo 1000 MHz ou superior.

Interfaces - Possuir no mínimo 7 interfaces de 1GB, 2 (duas) portas USB’s para expansão e 1 porta Console para gerenciamento.

Memória (RAM/Flash) - Possuir memória RAM de no mínimo 1,5 GB e memória flahs de 128MB ou superior.

Single Sign-On (SSO) Users. Deverá suportar um mínimo de 500 usuários autenticados na forma SSO.

VLAN Interfaces - Suporte ao número mínimo de 50 interfaces virtuais (VLAN interfaces)

Firewall Inspection Throughput .

Deverá apresentar Inspeção de firewall com Taxa de transferência de 1.300MBps ou superior.

Full DPI Throughput2 : Deverá apresentar

Inspeção profunda de pacotes (DPI) com Taxa de transferência de 400 MBps ou superior

IPS Throughput2: Deverá apresentar serviços de Prevençao de Instrusão, (IPS) com Taxa de

transferência de 1 Gbps ou superior.

Anti-malware Throughput2 : Deverá apresentar serviços de Anti-malware, (Anti-virus) com Taxa de transferência de 400MBps ou superior.

IPSec VPN Throughput3 : Deverá apresentar

serviço de VPN, no formato de IP Seguro (Ipsec), com Taxa de transferência de 900MBps ou superior.

Conexões por segundo: Suportar no mínimo 6.000 conexões por segundo.

Túneis de VPN Site-to-Site: Deverá implementar no mínimo de 20 Túneis VPN, do tipo Site-To-Site, já devidamente licenciado.

Clientes IPSec VPN : Suportar um mínimo

de 25 clientes VPN IPSEC.

Clientes SSL VPN: Suportar um mínimo

de 100 clientes VPN SSL.

Padrões de segurança: Deverá suportar a

formatos de critpografica: DES, 3DES, AES (128, 192, 256-bit), MD5, SHA-1, Suite B Cryptography Route-based VPN: Suportar o Modelos de roteamento RIP v1/v2, OSPF, rota estática, Roteamento baseado em política e Multicast.

Certificate Support Deverá possuiir certificação com os provedores Verisign, Thawte, Cybertrust, RSA Keon, Entrust.

VPN Features : Deverá possuir os recursos de

VPN nativos, Dead Peer Detection, DHCP Over

VPN, IPSec NAT Traversal, Redundant VPN

Gateway, Route-based VPN

Plataformas suportadas de Cliente VPN: Deverá fornecer Cliente nativo do fabricante do appliance, para fins de conexão VPN, SSL/IPSEC.

O cliente deve ter compatibilidade com os Sistemas operacionais versão Windows 10 ou superior. (32 e 64 bits)

Conexão mobile: Deverá suportar conexão

através de dispositivo móvel, compativel com

Apple iOS, Mac OS X, Google Android e Windows.

O aplicativo para conexões mobile deverá estar disponível e sem custo para o usuário da solução.

DPI Services: Deverá apresentar os serviços

de Inspeção de Pacote Profunda (Gateway Anti- Virus, Anti-Spyware, Intrusion Prevention, DPI SSL).

Estas funções/ou funcionalidades deverão estar devidamente licenciadas por um período de 3 anos.

Content Filtering Service (CFS): Deverá

apresentar Serviço de Filtro de conteúdo Web, no seguintes formatos: HTTP URL, HTTPS IP,

palavra chave (keyword and content scanning),ActiveX, Java Applet, e Cookie blocking bandwidth management, e nas categorias de fitro ter a funçao de permitir e bloquear por lista. Esta função deverá estar devidamente licenciada por um período de 3 anos.

Serviço Anti-Spam: Deverá suportar Serviço

abrangente anti-spam.

Controle de aplicações: Deverá implementar

controle de aplicação, com possibilidade de

bloqueio por assinatura de aplicação. Esta função deverá estar devidamente licenciada por um período de 3 anos.

Atribuição de IP Address: Deverá implementar os serviços de atribuição de IP: estático, (DHCP, PPPoE, L2TP and PPTP client), DHCP server interno e DHCP relay.

NAT Modes : Deverá implementar os

serviços Tradução de Endereços de Rede : 1: 1, 1: muitos, muitos: 1, muitos: muitos NAT flexíveis (IPs sobrepostos), PAT e modo transparente.

QoS: Deverá implementar Prioridade de

largura de banda, largura de banda máxima,

largura de banda garantida, marcação DSCP,

802.1e (WMM).

Authentication: Deverá implementar os

padrões de autenticação XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, e até 150 usuários internos.

VoIP: Deverá implementar os padrões de

VOIP Full H.323v1-5, SIP Padrões: Deverá suportar os padrões TCP/IP, UDP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3

Certificaçõess: Deverá possuir as

certificações FIPS 140-2 (with Suite B) Level 2,

UC APL, VPNC, IPv6 (Phase 2), ICSA Network

Firewall, ICSA Anti-virus ou equivalentes.

Fator de forma: desktop Fonte de energia (W) Fonte: 24W externa, com entrada 100 a 240Volts AC.

Dimensões Dimensões do appliance padrão rack 19” (polegadas) máximo de 2(dois) U’s

Weight Peso máximo 2,5 kg

Ambiente: Deverá suportar temperatura

ambiente de até 40° C

Licenças/Suporte: "O appliance deverá estar

devidamente licenciado, por período de 03 anos, com os serviços de segurança do tipo Gateway Anti-Virus, Anti-Spyware, IPS, IDS, Application Intelligence Service. DPI, e Suporte direto com o fabricante.

• Atualizações de software e firmware e

Atualizações de segurança, baixadas direta e

automaticamente na base de dados do fabricante.

• Suporte 24 horas por dia, via bate-papo,

telefone, e-mail e web.

• Suporte para configuração básica e assistência de solução de problemas.

• Substituição avançada de harware (RMA) em caso de falha do appliance."

Relatórios - Deverá fornecer Software de Relatório analítico de Internet, acessível por interface WEB GUI, do tipo Syslog, com Relatórios gráficos completos, permitindo visibilidade e análise de ameaças/ataques e atividades de rede, possibilitando geração de relatórios programados universais, relatórios detalhados e relatórios rápidos, relatório baseado no usuário ou objeto, atividade, aplicações, uso de banda.

Deverá ser implementado na infraestrutura da contratante, sem consumir recursos de processamento do equipamento, no formato pre-configurado de Virtual Appliance, sem custos de licenciamento de sistema operacional convidado. Esta funcionalidade deverá ser fornecida já licenciada no appliance, com licença do tipo perpétua.

10- DETALHAEMNTO TÉCNICO MÍNIMO Licença de Software antivírus endpoint para estações e servidor período de 3 anos solução corporativa de prevenção de ameaças de nova geração – Especificações Mínimas

1. Plataforma

1.1. A console de administração deve ser centralizada, com administração individualizada para **Federação de Agricultura e Pecuária do estado de Rondônia - Faperon** , possibilitando gerenciar todos os endpoints, independentemente da localização geográfica deste;

1.2. A console de administração deve ser acessível em qualquer ponto da rede da contratante até mesmo quando estiverem conectados a redes públicas sem a necessidade de uma conexão VPN;

1.3. A administração deve estar acessível através de HTTPS através usando um dos avegadores abaixo:

1.4. Google Chrome;

1.5. Edge;

1.6. Firefox.

1.7. A administração da solução deverá ser 100% em nuvem sem a necessidade de instalação de ferramenta local para o gerenciamento da solução;

1.8. A plataforma em nuvem deverá ser atestada e garantir que utiliza controles de segurança, disponibilidade, integridade de processamento, confidencialidade ou privacidade das informações de acordo com os padrões estabelecidos na certificação SOC2 (Padrão de Controle mundial de Organização de Serviços com auditoria que garante que os provedores de serviços gerenciem dados com segurança, para proteger os interesses e a privacidade de seus usuários e clientes).

1.9. A gerência de administração da solução deve ter capacidade de separar os endpoints gerenciados através de grupo via seleção manual e também a criação de grupos com adição de endpoints de forma automática com base em no mínimo, os critérios abaixo:

1.9.1. Domínio;

1.9.2. Endereços IP Externo;

1.9.3. Endereço de rede Externo (CIDR);

1.9.4. Hostname parcial ou completo;

1.9.5. Endereços IP Local;

1.9.6. Endereço de rede local (CIDR);

1.9.7. Fabricante do dispositivo;

1.9.8. Modelo do dispositivo;

1.9.9. Plataforma;

1.9.10. Versão de sistema operacional;

1.9.11. Unidade Organizacional do Active Directory;

1.9.12. Marcações personalizadas (Tags);

1.9.13. Versão do agente.

1.10. A gerência deve permitir aplicação de políticas para grupos de máquinas ou máquinas individuais;

1.11. O uso de um fator de autenticação duplo deve ser utilizado para

autenticação na console de gerenciamento da solução;

1.12. Deve ser possível a definição de papéis (RBAC) para os usuários dentro da console de administração delimitando as permissões e/ou acesso as funcionalidades e capacidades disponíveis dentro da plataforma;

1.13. A console de gerenciamento deve oferecer suporte Single Sign On com compatibilidade de pelo menos 3 opções distintas de provedor de identidade (IdP) na qual uma das opções deve ser obrigatoriamente Active Directory, sendo que essa opção deverá suportar tanto Active Directory Federation Services (AD FS) quanto Azure Active Directory (Azure AD);

1.14. A console deve contemplar, no mínimo, as seguintes visualizações:

1.14.1. Agentes ativos;

1.14.2. Agentes por sistema operacional;

1.14.3. Detecções por objetivo do ataque;

1.14.4. Detecções por tática do ataque;

1.14.5. Detecções por severidade do ataque;

1.14.6. Top 10 de detecções por máquina;

1.14.7. Top 10 de detecções por usuário;

1.14.8. Top 10 de detecções por arquivos;

1.15. A gerência da solução deve prover auditoria detalhada com, no mínimo, as seguintes ações administrativas:

1.15.1. Criação de grupos;

1.15.2. Adição de exclusões;

1.15.3. Autenticação por SSO;

1.15.4. Autenticação de usuário;

1.15.5. Autenticação de dois fatores;

1.15.6. Troca de senha da interface de gerenciamento;

1.15.7. Criação de usuários;

1.15.8. Deletar grupos;

1.15.9. Deletar políticas;

1.15.10. Revelar senha para desinstalação;

1.15.11. Iniciar isolamento de rede;

1.15.12. Atualizar permissões de usuário;

1.16. A console de administração deve centralizar a administração dos

sistemas operacionais Windows, Mac OS e Linux, não sendo aceitas múltiplas consoles para administração;

1.17. A console de gerência central deve ser capaz de atualizar os agentes de forma automática definida via política considerando no mínimo as seguintes opções:

1.17.1. Versão mais recente;

1.17.2. Versão específica;

1.17.3. Uma versão anterior a mais recente (N-1);

1.17.4. Duas versões anteriores a mais recente (N-2).

1.17.5. A console de gerenciamento deve permitir criação de alertas para envio de e-mail para administradores.

2. Serviço de investigação e detecção de ameaças

2.1. A solução deve ser fornecida com serviço gerenciado de detecção de adversário infiltrados no ambiente e acionamento imediato do cliente via console e notificação por e-mail com recomendações de configuração para prevenção de atividade maliciosa;

2.2. O Serviço deve analisar campanhas de malwares e de incidentes gerados na console de administração;

2.3. O Serviço deve ser realizado através de análise humana e continua, 24x7, em busca de anomalias e estratégias de atacantes que fogem do escopo de tecnologia de segurança padrão;

2.4. A equipe especializada em Hunting deve ser de diferentes áreas de atuação, como: Governo, Empresa comercial, comunidade de inteligência e defesa;

2.5. O serviço deve ser fornecido pelo mesmo fabricante da plataforma ofertada, não sendo aceito nenhum tipo de integração externa ou automatização de detecção e investigação;

2.6. O serviço deve ser disponibilizado 24x7 tendo atuação em qualquer horário;

2.7. O Serviço deve fornecer notas explicativas ou recomendações para

remediação baseado nas atividades encontradas;

2.8. A solução deve notificar por e-mail os incidentes;

2.9. Capacidade de processamento de dados massivos em busca de atividades maliciosas;

2.10. Capacidade de reportar informações referente ao incidente na própria console de administração;

2.11. A equipe especializada deve realizar busca história de dados em busca de evidências de intrusão;

2.12. A solução deve fornecer as seguintes dashboards:

2.12.1. Total de indícios de ameaças geradas;

2.12.2. Total de indícios de ameaças investigadas;

2.12.3. Total de incidentes acionados;

2.12.4. Total de detecções acionadas;

3. Características dos Agentes/ Sensores para estações de trabalho

3.1. A solução deve possuir um único software agente instalado em cada endpoint para prover todas as funcionalidades descritas neste documento e que serão administradas através da conexão com a console de gerenciamento. Não será aceita a instalação de componentes adicionais como agentes de comunicação com múltiplos subagentes, plug-ins e softwares de terceiros para o atendimento dos requisitos;

3.2. O agente deve suportar os sistemas seguintes sistemas operacionais:

3.2.1. Windows Server 2019;

3.2.2. Windows Server 2016;

3.2.3. Windows Server 2012 R2;

3.2.4. Windows Server 2012;

3.2.5. Windows Server 2008 R2 SP1;

3.2.6. Windows Server Core 2019;

3.2.7. Windows Server Core 2016;

3.2.8. Windows Storage Server 2012 R2;

3.2.9. Windows 10;

3.2.10. Windows 8.1;

3.2.11. MacOS Big Sur 11.0;

3.2.12. MacOS Catalina 10.15 ou posterior;

3.2.13. MacOS Mojave 10.14 ou posterior;

3.2.14. Amazon Linux 2;

3.2.15. Amazon Linux AMI 2018.03;

3.2.16. Amazon Linux AMI 2017.09;

3.2.17. Amazon Linux AMI 2017.03;

3.2.18. CentOS 7.4 - 7.7;

3.2.19. CentOS 6.7 - 6.10;

3.2.20. CentOS 8.0, 8.3, 8.2, 8.3;

3.2.21. Oracle Linux 6 - UEK 3, 4;

3.2.22. Oracle Linux 7 - UEK 3, 4, 5 e 6;

3.2.23. Oracle Linux 8 – UEK 6

3.2.24. Red Hat Enterprise Linux (RHEL) 7.4 - 7.7;

3.2.25. Red Hat Enterprise Linux (RHEL) 6.7-6.10;

3.2.26. Red Hat Enterprise Linux (RHEL) 8.0;

3.2.27. SUSE Linux Enterprise 15;

3.2.28. SUSE Linux Enterprise 12.2 - 12.5;

3.2.29. SUSE Linux Enterprise 11.4;

3.2.30. Ubuntu 18-AWS;

3.2.31. Ubuntu 18.04 LTS;

3.2.32. Ubuntu 16-AWS;

3.2.33. Ubuntu 16.04 LTS;

3.3. O agente deve trazer suportabilidade para Docker.

3.4. A comunicação entre os agentes e a console de gerenciamento deve utilizar um túnel de segurança TLS criptografado utilizando certificate pinning;

3.5. O agente deve suportar comunicação com a console de gerenciamento através de proxy;

3.6. Características específicas para sistemas operacionais Windows 3.6.1. O agente deve implementar proteção de desinstalação através de senha ou token específica para cada endpoint gerenciado.

3.6.2. O agente deve conter mecanismos que garantam que seu funcionamento não possa ser interrompido por usuários sem privilégios administrativos;

3.6.3. Deve detectar tentativas de manipulação indevida dos componentes do agente;

3.6.4. Deve incorporar técnicas de aprendizado de máquina (Machine Learning) para detecção e prevenção de ataques;

3.6.5. Não serão aceitas soluções que utilizem somente assinaturas para reconhecer ameaças;

3.6.6. Deve permitir níveis de sensibilidade diferentes para detecção e prevenção de ataques através do componente de aprendizado de máquina;

3.6.7. Deve ser capaz de detectar Adware e programas potencialmente indesejados;

3.6.8. Deve ser capaz de detectar ameaças mesmo que o endpoint não esteja conectado à Internet;

3.6.9. Deve permitir bloqueio personalizado através da inclusão de assinaturas digitais (hashes) de arquivos;

3.6.10. Deve permitir bloqueio de scripts e comandos em PowerShell considerados suspeitos;

3.6.11. Deve permitir bloqueio automático de processos suspeitos;

3.6.12. Deve permitir bloqueio baseado em análise do centro de inteligência do fabricante;

3.6.13. Deve permitir bloqueio de operações em registro suspeitas;

3.6.14. Deve permitir que arquivos maliciosos possam ser movidos para uma área de quarentena;

3.6.15. Deve possuir integração com o Windows Security Center para ser reconhecido como uma solução de proteção válida para antimalware;

3.6.16. Deve ser capaz de forçar a utilização de ASLR, de modo a mitigar ataques que exploram corrupção de memória;

3.6.17. Deve ser capaz de forçar Data Execution Prevention de forma a impedir ataques que utilizem espaço de memória para execução de códigos em região de memória não executável;

3.6.18. Deve ser capaz de impedir ataques que utilizem a técnica de Heap Spray Preallocation;

3.6.19. Deve ser capaz de impedir ataques que sobrescrevam SEH (Structured Exception Handling);

3.6.20. Deve ser capaz de detectar malwares do tipo Ransomware com

base em, no mínimo, os comportamentos abaixo:

3.6.20.1. Deletar backups;

3.6.20.2. Operações em excesso ao sistema de arquivos;

3.6.20.3. Criptografia de arquivos;

3.6.20.4. Processos associados a malwares de ransomware Cryptowall,

Wannacry, Locky;

3.6.21. Deve ser capaz de detectar exploração baseado em, no mínimo, os seguintes comportamentos:

3.6.21.1. Criação de processos suspeitos originados de navegadores;

3.6.21.2. Detecção de comprometimento de servidores Web através de webshell;

3.6.21.3. Detecção de arquivos suspeitos baixados ou escritos por um navegador que iniciaram a sua execução;

3.6.21.4. Injeção de código não esperada de um processo a outro;

3.6.21.5. Execução de JavaScript através do executável Rundll32.

3.6.22. Deve ser capaz de detectar movimentação lateral através de circunvenção do processo de logon do Windows;

3.6.23. Deve ser capaz de detectar de processos que tentam obter

credenciais de login;

3.6.24. A solução deverá ter sido avaliada pelo MITRE e atender ao menos as seguintes técnicas dentro da avaliação do MITRE ATT&CK: 3.6.24.1. T1088, T1086, T1059, T1056, T1110, T1071, T1061, T1055, T1081, T1022, T1048, T1083, T1222, T1050, T1126, T1057, T1012, T1060, T1076, T1105, T1018, T1204, T1053, T1035, T1071, T1033, T1078,.

3.6.25. Deve permitir que administradores possam executar ações de remediação remotamente, sem necessidade ou integração com soluções de terceiros e sem a instalação de softwares adicionais no endpoint gerenciado;

3.6.26. Deve permitir exclusão de arquivos e pastas utilizando caracteres

coringa (Wildcard);

3.6.27. Deve permitir a definição granular da execução ou não de, no mínimo, os seguintes comandos de alto risco sendo executados de forma remota no endpoint via console de gerenciamento:

3.6.27.1. Extração de arquivos;

3.6.27.2. Envio de arquivos para um repositório externo;

3.6.27.3. Iniciar execução de um processo;

3.6.27.4. Dump de memória do endpoint;

3.6.27.5. Dump de memória de um processo específico no endpoint.

3.6.28. Deve permitir que scripts PowerShell possam ser adicionados à solução para que possam ser executados remotamente em resposta à um incidente de segurança;

3.6.29. Deve permitir que o acesso remoto seja desabilitado globalmente

em endpoints específicos;

3.6.30. Deve implementar permissões específicas de forma a impedir que

o acesso remoto esteja disponível somente para usuários específicos;

3.6.31. Deve permitir que administradores possam interromper tráfego de

rede de endpoints classificados como comprometidos, restringindo a comunicação somente com a console de gerenciamento;

3.6.32. Possuir a capacidade de adição de endereços específicos para mesmo quando o endpoint esteja em quarentena sejam alcançáveis, ou seja, quando houver o isolamento do endpoint o mesmo deverá ter a possibilidade de comunicar com endereços especificados em política ademais da comunicação com a console de gerência;

3.6.33. Deve permitir que proteção de dispositivos seja habilitada em modos de detecção somente, sem bloqueio efetivo;

3.6.34. Deve permitir bloqueio de dispositivos USB baseado em, no mínimo, as seguintes classes de dispositivo:

3.6.34.1. Dispositivos de imagem;

3.6.34.2. Dispositivos de áudio e vídeo;

3.6.34.3. Dispositivos de armazenamento em massa;

3.6.34.4. Dispositivos móveis (MTP/PTP)

3.6.34.5. Impressoras;

3.6.34.6. Adaptadores de rede wireless;

3.6.35. Para dispositivos de armazenamento em massa, deve permitir

acesso granular com no mínimo, as seguintes permissões:

3.6.35.1. Leitura somente;

3.6.35.2. Escrita e leitura;

3.6.35.3. Escrita leitura e execução;

3.6.35.4. Bloqueio total;

3.6.36. A proteção de dispositivos deve permitir exceções baseadas no Vendor ID e Product ID, número serial e classe;

3.6.37. Deve permitir a criação de regras, grupos de regras e políticas de firewall para definir com precisão qual tráfego de rede é permitido e bloqueado no host;

3.6.38. A política de firewall deve permitir a utilização de múltiplas regras de firewall;

3.6.39. As regras de firewall devem ser agrupáveis, ou seja, as regras de firewall utilizadas em uma política devem ser configuradas de forma a ser possível de selecionar um grupo de regras a serem usadas em uma política;

3.6.40. Regras de firewall devem suportar minimamente as seguintes características:

3.6.40.1. IPv4;

3.6.40.2. IPv6;

3.6.40.3. Protocolos:

3.6.40.4. Any;

3.6.40.5. TCP;

3.6.40.6. UDP;

3.6.40.7. ICMP;

3.6.40.8. Avançado (permitindo especificar o número do protocolo).

3.6.40.9. Endereço local;

3.6.40.10. Porta local;

3.6.40.11. Endereço remoto;

3.6.40.12. Porta remota;

3.6.40.13. Ação:

3.6.40.14. Permitir;

3.6.40.15. Bloquear.

3.6.40.16. Direção da conexão:

3.6.40.16.1. Inbound;

3.6.40.16.2. Outbound;

3.6.40.16.3. Inbound ou Outbound.

3.6.41. Perfil de rede (para que a regra seja aplicada de acordo com o perfil da interface de rede):

3.6.41.1. Domínio;

3.6.41.2. Privado;

3.6.41.3. Público.

3.6.41.4. Processo;

3.6.41.5. Deve ser possível a configuração de regras de firewall em modo observação, gerando assim registros de qual seria a ação/impacto caso a regra fosse aplicada;

3.6.42. As regras dentro de um grupo podem ser habilitadas ou desabilitadas de forma independente;

3.7. Características específicas para sistemas operacionais MAC

3.7.1. Deve incorporar técnicas de aprendizado de máquina (Machine Learning) para detecção de ataques;

3.7.2. Deve permitir níveis de sensibilidade diferentes para detecção e prevenção de ataques através do componente de aprendizado de máquina;

3.7.3. Deve ser capaz de detectar Adware e programas potencialmente indesejados;

3.7.4. Deve ser capaz de detectar ameaças mesmo que o endpoint não esteja conectado à Internet;

3.7.5. Deve permitir bloqueio personalizado através da inclusão de assinaturas digitais (hashes) de arquivos;

3.7.6. Deve permitir bloqueio automático de processos suspeitos;

3.7.7. Deve permitir bloqueio baseado em análise do centro de inteligência do fabricante;

3.7.8. Deve permitir que arquivos possam ser movidos para uma área de quarentena;

3.7.9. Deve permitir bloqueio de utilização suspeita do modelo XPCOM;

3.7.10. Deve permitir bloqueio de processos que se assimile ao comportamento do backdoor Empyre;

3.7.11. Deve permitir detecção de roubo de credenciais através coleta de hashes e através de monitoramento de configurações de login automático.

3.7.12. Deve permitir que administradores possam executar ações de remediação remotamente, sem necessidade ou integração com soluções de terceiros e sem a instalação de softwares adicionais no endpoint gerenciado;

3.7.13. Deve permitir que administradores possam interromper tráfego de rede de endpoints classificados como comprometidos, restringindo a comunicação somente com a console de gerenciamento;

3.8. Características específicas para sistemas operacionais Linux

3.8.1. Deve incorporar técnicas de aprendizado de máquina (Machine Learning) para detecção e prevenção de ataques;

3.8.2. Deve permitir níveis de sensibilidade diferentes para detecção e prevenção de ataques através do componente de aprendizado de máquina;

3.8.3. Deve permitir níveis de sensibilidade diferentes para detecção de ataques através do componente de aprendizado de máquina;

3.8.4. Deve permitir bloqueio personalizado através da inclusão de assinaturas digitais (hashes) de arquivos;

3.8.5. Deve permitir que administradores possam executar ações de remediação remotamente, sem necessidade ou integração com soluções de terceiros e sem a instalação de softwares adicionais no endpoint gerenciado;

3.8.6. Deve permitir que administradores possam interromper tráfego de rede de endpoints classificados como comprometidos, restringindo a comunicação somente com a console de gerenciamento;

3.9. Capacidades de inteligência de ameaças

3.9.1. O fornecedor deverá emitir alertas e relatórios periódicos sobre ameaças e contextos políticos e globais que possam influenciar na incidência de ataques de cibersegurança;

3.9.2. A inteligência de ameaças deve mapear campanhas de ataque e dar visibilidade de países e indústrias alvo, pais de origem da campanha e última atividade;

3.9.3. Para campanhas de ameaça, a inteligência de ameaças deve fornecer, quando aplicável, informações tais como vulnerabilidades utilizadas, métodos de instalação, ações e objetivos, métodos de entrega e breve descrição da campanha;

3.9.4. Deve associar, quando pertinente, detecções presentes no ambiente à campanha de ataques;

3.9.5. Deve permitir extração de indicadores de comprometimento como hashes MD5, SHA1, SHA256, domínios, endereços IP, endereços de email, nomes de arquivos associados às atividades maliciosas;

3.9.6. Deve permitir que administradores sejam notificados por email para cada emissão de relatório de inteligência de ameaças.

3.10. Capacidades de emulação de execução de código

3.10.1. A solução deve prover, integrada à console de administração, capacidades de emulação de execução de arquivos, sem instalação de

componentes adicionais ou softwares de terceiros;

3.10.2. Deve se integrar ao agente instalado em endpoints para permitir que arquivos suspeitos sejam enviados de forma automática ao serviço de emulação de execução;

3.10.3. A solução deve emular execução, no mínimo, nos seguintes

sistemas operacionais:

3.10.3.1. Windows 7 (32 e 64 bits);

3.10.3.2. Windows 10;

3.10.3.3. Linux Ubuntu;

3.10.3.4. Android.

3.10.4. A solução deve incluir na análise de execução, no mínimo, as seguintes características:

3.10.4.1. Táticas e técnicas de acordo como modelo de ameaças MITRE ATT&CK;

3.10.4.2. Caraterísticas comportamentais suspeitas;

3.10.4.3. Imagens de execução, quando aplicável;

3.10.4.4. Detalhes do arquivo como nome, hash, tamanho, tipo;

3.10.4.5. Atividade de rede incluindo conexões, endereços IP de destino,

domínios, portas;

3.10.4.6. Leitura e escrita de arquivos em disco;

3.10.4.7. Leitura e alteração de chaves de registro;

3.10.4.8. Detalhes de processos iniciados durante a execução.

3.11 Capacidades de detecção, visibilidade e investigação

4.1.1. As informações de telemetria dos incidentes e ações ocorridas nos endpoints deverão estar disponíveis na console centralizada independentemente do status operacional dos endpoints, ou seja, caso o endpoint esteja inoperante, a investigação dos incidentes e eventos deverá ser possível;

4.1.2. A solução deve ser capaz de coletar e enviar à console de gerenciamento os dados de telemetria das ações realizadas nos endpoints incluindo, no mínimo, as seguintes atividades:

4.1.2.1. Endereços de rede obtidos;

4.1.2.2. Login de usuários;

4.1.2.3. Informações de sistema operacional, modelo e última atividade;

4.1.2.4. Número de executáveis únicos;

4.1.2.5. Processos que foram executados;

4.1.2.6. Utilização de ferramentas administrativas;

4.1.2.7. Requisições DNS;

4.1.2.8. Conexões de rede incluindo portas e processos associados;

4.1.2.9. Arquivos compactados escritos;

4.1.2.10. Scripts escritos em disco;

4.1.2.11. Mapa de geolocalização de conexões de rede.

4.1.3. Deve permitir visibilidade sobre parâmetros de execução de um processo;

4.1.4. A solução deve permitir busca dos metadados coletados através de sintaxes que filtrem a busca, concatenando critérios;

4.1.5. Deve permitir a busca por hashes MD5 e SHA256;

4.1.6. Deve permitir buscas por nomes de arquivo;

4.1.7. Deve permitir a busca por atividades de usuário;

4.1.8. Deve permitir extração de dados em formato CSV e JSON.

3Relatórios e dashboard

5.1.1. A solução deverá prover Dashboard trazendo as detecções mais recentes, número de novas detecções e detecções por táticas nos últimos 30 dias.

5.1.2. A plataforma deverá ter a capacidade de reportar as detecções de forma agrupada tendo como opções de agrupamento no mínimo os seguintes critérios:

5.1.2.1. Por máquina;

5.1.2.2. Por tática;

5.1.2.3. Por técnica;

5.1.2.4. Por Severidade.

5.1.3. A plataforma deverá ter a capacidade de reportar as detecções, permitindo organizar com a mais recente no topo, ou a mais antiga no topo.

5.1.4. A plataforma deverá ter a capacidade de reportar as detecções, permitindo filtrar minimamente com base aos seguintes filtros:

5.1.4.1. Severidade;

5.1.4.2. Tática;

5.1.4.3. Técnica;

5.1.4.4. Usuário;

5.1.4.5. Host;

5.1.4.6. Tipo de sistema operacional;

5.1.4.7. Versão do sistema operacional;

5.1.4.8. Última hora;

5.1.4.9. Último dia;

5.1.4.10. Última semana;

5.1.4.11. Últimos 30 dias;

5.1.4.12. Nome de arquivo;

5.1.4.13. Hash do processo.

5.1.5. A solução deve prover a capacidade de relatório de todas as conexões remotas realizadas desde a console de gerenciamento ao endpoint gerenciado contendo minimamente as seguintes informações que não deverão ser passiveis de exclusão ou limpeza, garantindo assim o nãorepudio:

5.1.5.1. Login do administrador/operador que realizou a operação;

5.1.5.2. Nome do endpoint;

5.1.5.3. Duração da sessão;

5.1.5.4. Data e hora do início da sessão;

5.1.5.5. Arquivos copiados desde a máquina;

5.1.5.6. Comandos executados na máquina;

5.1.5.7. Caminho completo do arquivo copiado da máquina;

5.1.5.8. Data e hora de cada comando executado.

5.1.6. A plataforma deverá gerar relatório das máquinas contendo minimamente as seguintes informações, podendo ser exportada em CSV:

5.1.6.1. Hostname;

5.1.6.2. Data e hora da primeira comunicação;

5.1.6.3. Data e hora da última comunicação;

5.1.6.4. Versão do sistema operacional;

5.1.6.5. Modelo;

5.1.6.6. Tipo;

5.1.6.7. Unidade organizacional (OU);

5.1.6.8. Site;

5.1.6.9. Política de proteção aplicada;

5.1.6.10. Política de resposta aplicada;

5.1.6.11. Política de atualização aplicada;

5.1.6.12. Política de controle de dispositivos USB aplicada;

5.1.6.13. Política de firewall aplicada;

5.1.6.14. Identificação do host (UID/GUID);

5.1.6.15. IP local da máquina;

5.1.6.16. IP público da máquina;

5.1.6.17. MAC Address;

5.1.6.18. Versão do sensor/agente instalado.

5.1.7. O relatório de máquinas deverá ter a capacidade de aplicar filtros para inclusão ou exclusão de dados no relatório, considerando minimamente as seguintes opções de filtro:

5.1.7.1. Domínio;

5.1.7.2. Grupo;

5.1.7.3. Identificação do host (UID/GUID);

5.1.7.4. Hostname;

5.1.7.5. IP local da máquina;

5.1.7.6. MAC Address;

5.1.7.7. Subnet da máquina;

5.1.7.8. Versão do sistema operacional;

5.1.7.9. Unidade organizacional (OU);

5.1.7.10. Plataforma;

5.1.7.11. Política de proteção aplicada;

5.1.7.12. Política de resposta aplicada;

5.1.7.13. Política de atualização aplicada;

5.1.7.14. Versão do sensor/agente instalado.

5.1.8. Deverá apresentar dashboard contendo minimamente as seguintes informações:

5.1.8.1. Total de hosts vistos nas últimas 24 horas;

5.1.8.2. Total de estações vistos nas últimas 24 horas;

5.1.8.3. Total de servidores vistos nas últimas 24 horas;

5.1.8.4. Hosts comunicando na última hora;

5.1.8.5. Hosts off-line;

5.1.8.6. Hosts isolados/quarentenados;

5.1.8.7. Hosts com sensor sem proteção para desinstalação;

5.1.8.8. Total de máquinas em cada política de proteção;

5.1.8.9. Total de máquinas em cada política de resposta;

5.1.8.10. Total de máquinas em cada política de atualização do sensor;

5.1.8.11. Total de máquinas em cada política de controle USB;

6. Suporte especializado do fabricante das soluções

6.1.1. Possuir portal de suporte para abertura de chamados, acesso a base de conhecimento;

6.1.2. O suporte deverá atender via telefone em escala 24x7x365;

6.1.3. Gerenciamento proativo de chamados;

6.1.4. Relatórios trimestrais;

6.1.5. Revisão trimestral de saúde do ambiente;

6.1.6. Apresentação de Roadmap;

6.1.7. O suporte deverá prover minimamente os seguintes canais de comunicação para abertura de chamados:

6.1.7.1. Chat;

6.1.7.2. Portal web.

6.1.8. O fabricante deverá realizar sessão de apresentação do serviço de suporte contemplando minimamente os seguintes tópicos:

6.1.8.1. Processo de abertura de chamado;

6.1.8.2. Processo de escalamento de chamado;

6.1.8.3. Recomendações e melhores práticas especificas para o ambiente

11- Licença pacote office Business 2021 formato ESD PN: T5D-03487

12- Impressora multifuncional Jato de Tinta tanque externo

Especificações Técnicas mínimas:

- Tecnologia de impressão: Jato de tinta Heat-Free MicroPiezo
- Resolução mínima de impressão: 5760 x 1440
- Velocidade mínima de impressão: 30 ppm em preto e 15 ppm em cores
- Deverá acomompanhar Cabo USB
- Capacidade mínima de Entrada do papel: 100 folhas de papel A4
- Capacidade mínima de Saída do papel: 30 folhas de papel A4
- Deverá suportar os seguintes formatos de papel padrão: A4, Carta, Ofício (215.9 x 355.6mm), Mexico-Oficio (215.9 x 340.4mm), Oficio 9 (214.9 x 315mm), Fólio (215.9x330.2mm), Executivo, Meia carta, A6
- Foto: 10x15 cm (4x6 in), 16:9 wide (102x181 mm), 13x18 cm (5x7 in)

- Envelopes: #10
- Definido pelo Usuário: 54x86 to 215.9x1200 mm
- Tipos de papel suportados: Comum e Papéis Especiais
- Resolução mínima do scanner: 1200 x 2400 dpi
- Profundidade mínima do scanner: 48-bit interna (24-bit externa)
- Área de escaneamento mínimo : 21,6 x 29,7 cm
- Velocidade minima de escaneamento: 12 segundos por página em preto e 30 segundos por página em cores (200 dpi)
- Tipos de Conexões: USB 2.0 de alta velocidade / Wireless / Wi-Fi Direct
- Suportar Voltagem: AC 100 - 240 V / 50 - 60 Hz
- Consumo elétrico maximo: 15 W em operação e 0,9W em repouso

Deverá acompanhar:
- 1 kit de garrafas originais (Preto, Ciano, Magenta e Amarelo)
- Cabo de alimentação
- Cabo USB
- CD de instalação e Softwares em português
- Guia de instalação rápida
- Certificado de Garantia do Produto
- Instrução para cadastro de garantia estendida se houver

Garantia mínima de : 12 meses

13- Nobreak com potência mínima de 2200VA e 1300W (Entrada Bivolt, Saída 115V), com possibilidade de expansão, USB/Serial, com no minimo 10 tomadas NBR 14136

Possuir capacidade Expansão de autonomia
Possuir Fusível com dispositivo rearmável
Possuir Saídas USB e RS232 para gerenciamento do UPS

Possuir no mínimo 6 tipos de Proteção:
Curto circuito no inversor;
Surtos de tensão (entre fase e neutro);
Sub/sobretensão da rede elétrica. Na ocorrência destas, o UPS passa a operar em modo bateria;
Sobreaquecimento no inversor e no transformador, com alarme e posterior desligamento automático;
Potência excedida, com alarme e posterior desligamento automático;
Descarga total das baterias.

Características de Entrada
Tensão nominal (Volts): 115/127/220 (automático)
Faixa de tensão de entrada para regulação de saída (Volts): 89 a 138 (rede 115/127V~); 175 a 255 (rede 220V~)

Faixa de tensão para operação em rede (Volts): 89 a 143 (rede 115/127V~); 175 a 255 (rede 220V~)
Frequência nominal (HZ): 60 ± 4

Conexão de Entrada
Cabo com plugue Padrão NBR14136 (20A)
Comprimento do cabo de força (mm): 1900 ± 50

Potência de Saida
Mínimo 2200VA/1300W
Fator de potência mínimo de: 0,60

Características de Saída
Tensão nominal (Volts): 115
Regulação de saída: ± 5% (para operação bateria); + 6% - 10% (para operação rede)
Frequência nominal (Hz): Configurável em 50/60 (padrão configurado de fábrica: 60)
Faixa de frequência (Hz): 60 ± 1% (para operação bateria)
Acionamento do inversor:< 0,8 ms
Forma de onda no inversor: Senoidal por aproximação (retangular PWM – controle de largura e amplitude)

Conexão de Saída
Mínimo de 10 tomadas, sendo: 6 tomadas de (10A) + 4 tomada de (20A)
Padrão das tomadas NBR 14136 - 3 pinos - Brasil

Baterias
Mínimo de Baterias internas: 2 baterias 12Vdc / 17Ah (24Vdc)

Permitir expansão de baterias externas
Possuir Conexão de baterias externas com conector de engate rápido

Mínimo de Recursos
Estabilizador interno com 4 estágios de regulação.
Filtro de linha interno.
Bargraph de LEDs que indica o nível de carga da bateria ou a potência de saída.
Autoteste ao ser ligado, o UPS testa todos os circuitos internos, inclusive as baterias.
Posusir sistema de autodiagnóstico de bateria: informa quando a bateria precisa ser substituída.
Possuir recarga automática das baterias.
Permitir ser ligado na ausência de rede elétrica (DC Start).
Possiir Função RMS que analisa os distúrbios da rede elétrica e possibilita a atuação precisa do UPS. Indicada principalmente para redes instáveis.
Permitir ligar no mínimo 2 módulos de bateria externa.

Gerenciamento

Serial RS-232 (Padrão ponto-a-ponto)
USB (Tipo A-B) deverá acompanhar cabo USB
Permitir gerenciamentp através de software do próprio fabricante.

Gabinete do Nobreak
Formato padrão: Torre
Dimensões maximas (A x L x P): 320 x 200 x 500 mm
Peso líquido máximo com embalagem: 40kg
Ruído audível: ≤60 dB a 1 metro de distância

14- TELA DE PROJEÇÃO ELÉTRICA TENSIONADA 16:9 WIDE SCREEN 150” POLEGADAS 3,32 M X 1,87

Detalhamento técnico mínimo

Dimensão, Largura total aproximada (de suporte a suporte): 3,77
Polegadas: 150"
Modelo: Elétrico
Altura total aproximada: 2,20
Formato: 16:9
Película da área de projeção: Matte White I
Fixação: Parede ou Teto
Enrolamento do tecido: Automático
Possuir Bordas negras nas laterais
Possuir Tensionamento nas laterais
Alimentação e Voltagem: 110v, 220v ou bivolt automático

15- TELA DE PROJEÇÃO ELÉTRICA PRIME 1:1 WSCREEN 110 POLEGADAS 2,00 M X 2,00 M

Detalhamento técnico mínimo

Dimensão, Largura total aproximada (de suporte a suporte): 2,28 m
Polegadas: 110
Modelo: Elétrico
Formato: 1:1
Película da área de projeção: Matte White I
Fixação: Parede ou Teto
Enrolamento do tecido: Automático
Possuir Bordas negras nas laterais
Possuir Tensionamento nas laterais
Alimentação e Voltagem: 110v, 220v ou bivolt automático

16- Impressora Laser Colorida

Especificações Técnicas

- Tecnologia de Impressão: Laser Eletrofotográfico
- Tela LCD (tipo/tamanho): Touchscreen Colorido de no mínimo 2,7”
- Tamanho do Papel suportado: Bandeja de Papel: Até 21,6 x 35,6 cm (Ofício) / Bandeja Multiuso: 7,6 - 21,6 cm (L) / 12,7 - 35,6 cm (C)
- Velocidade de Impressão de no minimo : 30 ppm em preto/cores
- Tempo de Impressão da 1ª Página: Menor de 15 segundos em preto/cores
- Resolução de Impressão: Até 2400 x 600 dpi
- Processador: 800 MHz ou superior
- Emulações: PCL6, BR-Script3, PDF versão 1.7, XPS Versão 1.0
- Possuir Capacidade de Impressão Frente e Verso
- Capacidade de Entrada de Papel minimo de: Bandeja para 250 folhas e uma bandeja multiuso para 50 folhas
- Capacidade de Entrada Opcional: 1.200 folhas com as bandejas opcionais
- Capacidade de Saída mínimo de : 150 folhas (face para baixo), 1 folha (face para cima)
- Tipos de Mídia suportados: Papel Comum, Timbrado, Papel Colorido, Papel Reciclado, Bond, Etiquetas e Envelopes (até 10)
- Gramaturas da Mídia suportados: Bandeja de papel padrão: 60 a 105 g/m² / Bandeja multiuso: 60 a 163 g/m²
- Memória padrão: 512 MB ou superior
- Interfaces Padrão de conexão: Wireless 802.11b/g/n, NFC+, Ethernet Gigabit, USB
- Sistemas Operacionais Compatíveis: Windows®: 10 Home, 10 Pro, 10 Education, 10 Enterprise, 8.1, 8, 7, Windows® Server2016, 2012 R2, 2012, 2008 R2, 2008, macOS v10.10.5, 10.11.x, 10.12, Linux
- Compatibilidade com Dispositivos Móveis: AirPrint™, Google Cloud Print™ 2.0, Brother iPrint&Scan, Mopria®, Wi-Fi Direct®, NFC+, Cortado Workplace
- Web Connect: GOOGLE DRIVE™, ONEDRIVE®, DROPBOX, BOX, ONENOTE®, EVERNOTE®
- Funções de Segurança: Leitor de Cartões NFC integrado, AcO ve Directory®, Secure Function Lock, Enterprise Security (802.1x), Impressão Segura, SSL/TLS, IPSec

Garantia mínima 12 Meses

9 - DOS CRITÉRIOS DE ELABORAÇÃO DA PROPOSTA E DA FORMA DE ADJUDICAÇÃO

9.1. Na elaboração da proposta deverão estar inclusos os custos diretos e indiretos inerentes aos procedimentos de entrega do bem a ser adquirido, tais como tributos,

serviços, encargos sociais, trabalhistas, frete, lucro e quaisquer outros necessários ao cumprimento integral do objeto.

9.2. Na proposta apresentada pelos fornecedores deverão constar o número do item, o quantitativo, o valor unitário e total de cada item, a descrição completa, a marca e o modelo/referência do produto ofertado.

9.4. Poderá solicitar ainda ao fornecedor informações mais detalhadas do objeto ofertado, podendo, inclusive, solicitar prospecto e catálogos oficiais do produto, assinalando prazo para apresentação, sob pena de recusa da proposta, bem como poderá solicitar a indicação dos sítios na internet dos fabricantes/importadores dos produtos.

7.5. Sagrar-se-á vencedor o fornecedor que ofertar o MENOR VALOR POR ITEM, e que atenda todas as exigências do presente termo.

8. PRAZOS PARA ENTREGA

8.1 O Prazo para entrega das mercadorias adquiridas, poderá ser permitida a **entrega em até 30 (trinta) dias úteis**, podendo ser prorrogado por no máximo 15 (quinze) dias úteis.

9. LOCAL E CONDIÇÕES DE ENTREGA DOS PRODUTOS

9.1 Fornecer todos os itens novos, sem uso anterior, os quais serão entregues na sede da **FAPERON**, localizado na Rua João Goulart, nº 1843, Bairro Nossa Senhora das Graças, CEP 76.804-126, Porto Velho – RO.

9.2 Todo e qualquer ônus decorrente da entrega do objeto, inclusive frete, será de inteira responsabilidade da CONTRATADA. A movimentação dos materiais até as dependências da FAPERON é de inteira responsabilidade da CONTRATADA ou da transportadora, não sendo a FAPERON responsável pelo fornecimento de mão de obra para viabilizar o transporte.

10 DO PAGAMENTO

10.1 O pagamento referente ao fornecimento dos materiais será efetuado através de transferência bancária (gerenciador financeiro), **após entrega dos itens** e a certificação da Nota Fiscal/Fatura pelo setor responsável, que deverá ser fornecida quando do recebimento Autorização de Fornecimento de Produtos expedido por esta FAPERON.

10.2 A nota fiscal será apresentada conforme **CNPJ: 04.918.215/0001-47** e deverá estar acompanhada por uma planilha detalhando os quantitativos e os materiais entregues.

10.3 As Notas Fiscais dos produtos deverão ser apresentadas acompanhadas das Certidões Negativas de Regularidade Fiscal Federal, INSS, FGTS, Estadual, Municipal e Trabalhista, dentro do prazo de validade, a FAPERON;

10.4 A nota fiscal que apresentar incorreções será devolvida para as devidas correções. Nesse caso, o prazo começará a fluir a partir da data de reapresentação da nota fiscal/fatura, sem incorreções.

11 OBRIGAÇÕES DA CONTRATADA

11.1 São obrigações da CONTRATADA:

11.2 Arcar com eventuais prejuízos causados à CONTRATANTE e/ou a terceiros, provocados por ação ou omissão do seu pessoal, na execução do fornecimento dos materiais contratados;

11.3 Prestar, quando solicitado, todos os esclarecimentos necessários;

11.4 Disponibilizar os materiais apenas mediante apresentação da Autorização de Fornecimento/ Ordem de Serviço emitida e assinada pelo gestor do contrato, representante da CONTRATANTE;

11.5 Indicar representante e um substituto (nos casos de ausência do representante nomeado) para relacionar-se com a entidade **FAPERON** como responsável pela execução do objeto, com acesso ao serviço de telefonia móvel celular para atender às solicitações da CONTRATANTE;

11.6 Não será permitido a CONTRATADA terceirizar o fornecimento do objeto sem que haja a autorização expressa da CONTRATANTE, permanecendo integralmente, responsável pela segurança e integridade física do bem contra danos materiais, incêndio, intempéries da natureza de qualquer espécie, independentemente da existência de culpa ou dolo, que venha atingir o patrimônio da FAPERON, de forma parcial ou total, não transferindo responsabilidade a subcontratada quando houver a autorização para a terceirização;

11.7 Manter durante a vigência do Contrato todas as condições de habilitação e qualificação exigidas.

11.8 A CONTRATADA assumirá integral responsabilidade pelo fornecimento dos materiais em eficiência, atendendo as especificações e quantidades definidas neste termo de referência.

11.9 A Empresa vencedora responsabilizar-se-á pelo fiel cumprimento de todas as condições estabelecidas no presente Termo, disposições e acordos relativos à legislação social, penal e trabalhista em vigor, particularmente no que se refere ao pessoal alocado para o fornecimento dos materiais contratados.

11.10 Toda e qualquer despesa com materiais, mão de obra, transportes, impostos, licenças, leis trabalhistas e outros encargos inerentes ao fornecimento dos materiais, ficará por conta da empresa CONTRATADA. Deverá também à mesma, possuir ferramentas apropriadas para a execução da entrega dos materiais, bem como EPIs (Equipamentos de Proteção Individual) para o prestador dos serviços de transporte e descarregamento dos materiais.

11.11 A CONTRATANTE não se responsabilizará por qualquer acidente provocado por funcionário ou prestador de serviço da empresa CONTRATADA, que porventura venha acontecer nas dependências do prédio ou fora dela, envolvendo pessoas, equipamentos do edifício, o próprio edifício, veículos ou qualquer tipo de objeto. Caso isso venha a acontecer, a empresa CONTRATADA deverá tomar todas as providências e providenciar os reparos sem ônus para a CONTRATANTE.

11.12 Responsabilizar-se pelos vícios e danos decorrentes do produto, de acordo com os artigos 12, 13, 18 e 26, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990);

11.13 dever previsto no subitem anterior implica na obrigação de, a critério da Administração, substituir, reparar, corrigir, remover, ou reconstruir, às suas expensas, no prazo máximo de 10 (dez) dias corridos, o produto com avarias ou defeitos;

12 DAS OBRIGAÇÕES DA CONTRATANTE

12.1 São obrigações da CONTRATANTE:

12.1.1 Exigir o cumprimento de todos os compromissos assumidos pela CONTRATADA, de acordo com as cláusulas contratuais e seus Anexos;

12.1.2 Efetuar o pagamento à CONTRATADA de acordo com o preço, os prazos e as condições estipuladas no contrato;

12.1.3 Prestar as informações e esclarecimentos que venham a ser solicitados pela empresa CONTRATADA e seus colaboradores;

12.1.4 Comunicar imediatamente à CONTRATADA qualquer irregularidade manifestada no fornecimento dos materiais;

12.1.5 Promover através de seu representante, o acompanhamento e a fiscalização do fornecimento dos materiais, sob os aspectos quantitativos e qualitativos, anotando em registro próprio as falhas detectadas e notificar à CONTRATADA por escrito, sobre as imperfeições, falhas, irregularidades ou ocorrências de quaisquer fatos relativos aos materiais adquiridos que, a seu critério, exijam medidas corretivas a serem adotadas por parte da CONTRATADA;

12.1.6 Receber os materiais sempre que atenderem aos requisitos do Contrato, do Termo de Referência e do Edital, ou indicar as razões da recusa.

13 DA DOTAÇÃO ORÇAMENTÁRIA

13.1 As despesas decorrentes da execução do objeto do presente Termo correrão a cargo da conta finalística do FAPERON e Elementos Orçamentários abaixo:

14 DA RESCISÃO CONTRATUAL

14.1. O contrato poderá ser rescindido nos termos do que dispõem a Regulamento de Licitações e Contratos do SENAR ou consultar a assessoria jurídica.

15 DO FORO

15.1. Fica eleito o foro da Comarca de Porto Velho, Rondônia, para dirimir questões oriundas deste instrumento, renunciando as partes a qualquer outro por mais privilegiado que seja.

Porto Velho/RO, 9 de novembro de 2022.

Rua João Goulart nº 1843 – Bairro: Nossa Senhora das Graças – E-mail: faperon@faperon.br
Telefone: (69) 32148371 - Cep: 76804-126 – Porto Velho - Rondônia