ANEXO I - TERMO DE REFERÊNCIA

PREGÃO ELETRÔNICO Nº 2/2025

1.DO OBJETO

1.1. **REGISTRO DE PREÇOS** para o fornecimento de equipamentos e programas de informática (servidores, equipamentos de redes, solução antivírus, microcomputadores, notebooks), e equipamentos de comunicação (projetores, telas de projeção e TVs de LED) para implementação da infraestrutura física dos Centros de Excelência, para uso administrativo e nas salas de aula, localizados nas cidades de Tangará da Serra/MT, Feira de Santana/BA e Ribeirão Preto/SP, conforme condições, especificações e quantitativos constantes neste Termo de Referência.

1.2. Os equipamentos e programas a serem adquiridos deverão seguir as normas e requisitos técnicos dos fabricantes e ABNT - Associação Brasileira de Normas Técnicas.

2. DA JUSTIFICATIVA

Visando melhorar a prestação dos nossos serviços e ampliar a capilaridade de atuação na área educacional e na assistência técnica rural, o Serviço Nacional de Aprendizagem Rural – Senar implantou uma rede física de ensino nacional distribuída estrategicamente em diversas unidades da federação, por meio da construção dos seus Centros de Excelência em Educação Profissional e Assistência Técnica Rural, vocacionados para a gestão e para as principais cadeias produtivas do agronegócio.

Está entre as atribuições do Senar Central equipar este Centro com o objetivo de ampliar seu portfólio educacional, por meio da oferta de cursos técnicos de nível médio, presencial e a distância, bem como aprimorar e assegurar a qualidade dos serviços realizados, expandindo a estrutura organizacional de suas Regionais.

3. DA ACEITABILIDADE DOS EQUIPAMENTOS

3.1. Os equipamentos e programas de informática serão especificados em lotes, de acordo com as suas características e finalidades a que se destinam, para manter a padronização de fornecedores e fabricantes.

3.2. Todas as especificações dos equipamentos estão definidas como mínimas para serem aceitas pela área técnica, assim, as empresas licitantes poderão oferecer para apreciação e avaliação técnica, configurações superiores ao que está sendo solicitado.

3.3. As despesas com a entrega de todos os equipamentos e/ou materiais a serem adquiridos, serão de total responsabilidade da(s) licitante(s) vencedora(s).

4. DA HABILITAÇÃO TÉCNICA

4.1. Comprovação de aptidão para desempenho de atividade pertinente e compatível em características, quantidades e prazos com o objeto da licitação, por meio de 01 (um) ou mais atestado(s) fornecido(s) por pessoa jurídica de direito público ou privado, em conformidade com as especificações descritas nos subitens abaixo, contendo as seguintes informações:

a) Nome ou razão social, CNPJ e endereço completo do emitente;
b) Data de emissão do atestado ou da certidão;

Serviço Nacional de Aprendizagem Rural

www.senar.org.br

SGAN Quadra 601 Módulo K
Ed. Antônio Ernesto de Salvo
Brasília/DF - CEP 70.830-021
Telefone: (61) 2109-1400

c) Assinatura e identificação do signatário (nome, cargo e função que exerce junto à empresa emitente).

5. DAS ESPECIFICAÇÕES TÉCNICAS (EQUIPAMENTOS E PROGRAMAS)

LOTE I – SERVIDOR COM SUPORTE PARA 02 PROCESSADORES	
QUANTIDADE	**06**
AQUISIÇÃO IMEDIATA: 02 EM TANGARÁ DA SERRA/MT	**02**
Modelo	Equipamento servidor tipo Rack
Características gerais	Possuir baias para discos de 2,5" e mínimo de 5 discos; Possuir display frontal para monitoramento das condições de funcionamento dos principais componentes do servidor através da exibição de alertas de falha, tais como*: a. falhas de processadores, b. falhas de memória RAM, c. falhas de fontes de alimentação, d. falhas de disco rígido; e. falhas de refrigeração.* O projeto do gabinete deve ter qualidade fabril e ser concebido de modo a permitir o acesso/abertura e a retirada de discos, placas, ventoinhas, memórias, fontes, sem o uso de ferramentas "tool-less". Deve possuir em local de fácil acesso para facilitar a localização do produto, número de série e outras informações do produto. Deve possuir desenhos que de forma intuitiva demonstrem a função de cada porta de expansão/conexão. Possuir led que facilite a leitura do status do servidor. Possuir tampa protetora dos discos com chave. Possuir ventiladores hot-plug com redundância, configurados em sua totalidade para suportar a configuração máxima do equipamento.
Fontes de alimentação	Fontes de alimentação hot-plug em redundância (1+1); cada fonte de alimentação deve possuir: a. Potência de, no mínimo, 750 Watts. b. Eficiência energética de 94% (80Plus Platinum) quando em carga de 50%, suficientes para operação do servidor em sua configuração máxima; Suportar e operar nas faixas de tensão de entrada de 100-240 VAC em 60 Hz; Possuir LED indicador de status que permita monitorar e diagnosticar as condições de funcionamento da mesma; Cabos de alimentação com conector padrão IEC C13/C14 e amperagem compatível com a potência da fonte de alimentação;
Processador	Possuir 2 (dois) processadores de arquitetura x86-64 de mesmo modelo, projetados para utilização em servidores; Cada processador deve possuir as seguintes características técnicas: a. Arquitetura x86-64 com no mínimo 2,4 Ghz; b. Processador com no mínimo 10 núcleos; c. Memória cache de, no mínimo, 12 MB; d. Tecnologia de aceleração dinâmica através da elevação da frequência de clock nominal baseado na utilização dos núcleos do processador. Essa tecnologia deve ser nativa da arquitetura do processador e não deve ultrapassar os limites estabelecidos pelo fabricante;

Serviço Nacional de Aprendizagem Rural

www.senar.org.br

SGAN Quadra 601 Módulo K
Ed. Antônio Ernesto de Salvo
Brasília/DF - CEP 70.830-021
Telefone: (61) 2109-1400

	e. Tecnologia de ajuste dinâmico do consumo de energia através do controle do clock e voltagem do processador baseado na utilização da CPU; f. Controladora de memória integrada de 6 (seis) canais, compatível com DDR4 2666 MHz ou superior; O processador deve possuir instruções AVX e extensões de virtualização.
Performance	O modelo de servidor com os 2 (dois) processadores ofertados devem possuir índice de performance SPECint_rate_base2017 de 630 ou superior, auditado pelo Standard Performance Evaluation Corporation (SPEC); Não será aceito modelo de servidor cuja performance não esteja auditada pelo SPEC, resultados obtidos com a utilização de servidores em cluster e estimativas de resultado de performance.
Memória RAM	O servidor deve ser compatível com módulos DDR4 com as seguintes características técnicas: a. RDIMM (Registered) e LRDIMM (Load Reduced); b. Clocks de 2666 MHz, 2933 MHz; e c. Módulos single rank (1R), dual rank (2R) e quad rank (4R) ou superior; O servidor deve suportar escalabilidade mínima de 7698GB; Possuir 96GB (6X16gb) de memória RAM, provisionados por módulos DIMM RDIMM ECC ou LRDIMM ECC, dual rank (2R) ou quad rank (4R), com capacidade de, no mínimo, 16 GB e velocidade de 2666 MHz ou superior; suportar tecnologia de memória de espera através da reserva de rank distribuído nos módulos de memória (Memory Sparing ou equivalente); Suportar tecnologia SDDC ou Advanced ECC ou Chipkill para detecção e correção de falhas de chip e erros multi-bit.
Motherboard	A motherboard deve ser da mesma marca do fabricante do microcomputador, desenvolvida especificamente para o modelo ofertado. Não serão aceitas placas de livre comercialização no mercado; Os componentes removíveis da motherboard sem o uso de ferramentas e componentes hot-plug devem possuir identificação visual a fim de facilitar seu manuseio; Possuir no mínimo 12 (doze) slots DIMM de memória DDR4; O servidor deve possuir, no mínimo,3 (três) slots PCI-Express e, no mínimo, de 1 (uma) porta USB 3.0 interna.
BIOS	BIOS desenvolvida pelo mesmo fabricante do equipamento ou este fabricante deve ter direitos copyright sobre a mesma, comprovados através de atestado. Não será aceito equipamentos com BIOS em regime de OEM ou customizadas; A BIOS deve possuir a informação do número de série do equipamento e um campo editável que permita inserção de identificação customizada (Asset Tag). Ambas as informações devem ser passíveis de consulta via software de gerenciamento; Possuir chip de segurança TPM (Trusted Plataform Module) versão 1.2 para armazenamento de chaves criptográficas.
Portas de entrada/saída	Possuir as seguintes portas situadas na parte traseira do gabinete: no mínimo, 1 (uma) porta de vídeo VGA padrão DB-15; no mínimo, 2 (duas) portas USB 2.0 ou superior; no mínimo, 1 (uma) porta serial (DB-9); Possuir as seguintes portas situadas na parte frontal do gabinete: no mínimo, 1 (uma) porta de vídeo VGA padrão DB-15; Todas as portas devem possuir identificação de sua funcionalidade.

Serviço Nacional de Aprendizagem Rural

www.senar.org.br

SGAN Quadra 601 Módulo K
Ed. Antônio Ernesto de Salvo
Brasília/DF - CEP 70.830-021
Telefone: (61) 2109-1400

Network	Possuir interfaces de rede Ethernet com as seguintes características técnicas: no mínimo, 4 (quatro) interfaces de rede Gigabit Ethernet 10/100/1000 Mbps.
Controladora RAID	a. Suportar drives SSD (Solid-State Drive), HDD (Hard Disk Drive); b. Memória cache mínimo de 2 GB; c. Proteção da cache através de memória flash não volátil; d. Suportar RAID 0, 1, 5, 6, 10, 50 e 60 vias hardware; e. Possuir canais SAS 12 Gb/s, suficientes para suportar a quantidade máxima de discos do servidor; f. Permitir expansão de volumes de forma on-line; g. Permitir migração de RAID de forma on-line; h. Permitir implementação de drives hot-sparing no formato global e dedicado; i. Suportar tecnologia S.M.A.R.T.;
Armazenamento	Possuir no mínio 5 (cinco) discos 1.2TB 10K RPM SAS 12Gbps 512n 2.5, hot-plug.
Gerenciamento	Console remota. O servidor deve possuir conexão que permita o acesso à console do equipamento através da rede. Esta conexão deve possuir 1 (uma) interface 1 Gbps exclusiva. O acesso a console deve ser feito através de https ou 'software' proprietário, possuindo usuário e senha de conexão, com criptografia dos dados trafegados. Caso seja necessário 'software' proprietário, este deve ser entregue em quantidade suficiente para administrar todos os servidores fornecidos. No mínimo, as seguintes funções devem estar disponíveis na console remota a. Ligar/Desligar o equipamento. b. Acesso a 'BIOS' e/ou 'firmware' do equipamento. c. Acompanhamento de todo o processo de inicialização do equipamento. d. Instalação do sistema operacional, através da console remota Acesso a console gráfica. e. Failover Network
Compatibilidade com Sistema Operacional	O modelo do servidor ofertado deve estar certificado para o sistema operacional Windows Server 2022 x64 e Windows Server 2012 R2 x64, comprovado através do Windows Server Catalog da Microsoft;
Componentes e Acessórios	O fabricante do servidor deve disponibilizar na sua respectiva web site, download gratuito de todos os drivers, BIOS e firmwares dos componentes que compõem este servidor; Deverá ser fornecido kit de trilhos deslizante e braço organizador de cabos, ambos do mesmo fabricante do servidor ofertado, para fixação dos servidores em rack 19 polegadas padrão EIA-310D.
Sistema Operacional	O servidor deverá ser entregue sem Sistema Operacional.
Garantia e Níveis de Serviço (SLA)	
Período	A garantia do equipamento deverá ser on-site e de mínimo de 36 (trinta e seis) meses.
Certificação	**CERTIFICAÇÃO 1**: O fabricante dos equipamentos deverá estar relacionado na web site da EICC, http://www.eiccoalition.org/about/members **OU**

Serviço Nacional de Aprendizagem Rural

www.senar.org.br

SGAN Quadra 601 Módulo K
Ed. Antônio Ernesto de Salvo
Brasília/DF - CEP 70.830-021
Telefone: (61) 2109-1400

	apresentar o **Certificado da OHSAS 18001** válido, **OU** ainda, possuir a **certificação ISO 14001**. **CERTIFICAÇÃO 2:** A empresa vencedora deste lote deverá apresentar, do fabricante, **Certificação EPEAT** ou **certificação emitida pelo INMETRO** ou entidade credenciada por este Instituto, em conformidade com a **Portaria n.º 170, de 10 de abril de 2012**.
Atendimento	O atendimento deverá ser no regime de 7x24 a ser realizado diretamente pelo fabricante do equipamento ou pela contratada, caso o fabricante a tenha certificado para tal.
Cobertura	A garantia deverá cobrir todos os itens que compõem o equipamento.
Chamado	A abertura de chamados deverá correr através de chamada telefônica para o número fixo, regime 7x24. Opcionalmente os chamados poderão ser abertos através do site na Internet.
Compatibilidade	O equipamento ofertado deverá ser compatível com o sistema operacional Microsoft Windows Server 2012 x64 R2 e 2016 x64 R2 ou superior, Red Hat Enterprise Linux (RHEL) Version 7.0 ou superior e VMWare ESXi 6.5 ou superior.

LOTE II – EQUIPAMENTOS DE REDE	
ITEM 1 – SWITCHES 48 PORTAS	
QUANTIDADE	**24**
AQUISIÇÃO IMEDIATA: 08 EM TANGARÁ DA SERRA/MT	**08**
Características Gerais	Deverá possuir, no mínimo, 48 (quarenta e oito) portas ethernet 10/100/1000BASE-T com autosensing de velocidade, conectores RJ-45; Possuir, adicionalmente às portas especificadas no item anterior, no mínimo, 4 (quatro) slots SFP LAN Base; As interfaces 10/100/1000BASE-T deverão obedecer às normas técnicas IEEE802.3 (10BASE-T), IEEE802.3u (100BASE-TX), 802.3ab (1000BASE-T) e IEEE802.3x (Flow Control); Todas as portas Ethernet 10/100/1000BASE-T deverão suportar auto configuração de crossover (Auto MDIX); Todas as portas Ethernet 10/100/1000BASE-T deverão suportar configuração Half-Duplex e Full-Duplex, com a opção de negociação automática; Suportar Jumbo frames de no mínimo 9.216 bytes; Permitir montagem em rack padrão de 19 (dezenove) polegadas, possuindo, no máximo, 1 RU (uma unidade de rack) de altura. Deverão ser ofertados os acessórios necessários para a correta instalação; Possuir LEDs para a indicação do status e atividade das portas, além, do modo de operação full-duplex ou half-duplex; Deverá ser fornecido com documentação técnica e manuais que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização do equipamento.
Fonte de Alimentação	Possuir fonte de alimentação AC bivolt, com seleção automática de tensão (na faixa de 100 a 240V) e frequência de 50/60 Hz; Possuir alimentação elétrica capaz de suportar o equipamento com todas as funcionalidades especificadas;

Serviço Nacional de Aprendizagem Rural

www.senar.org.br

SGAN Quadra 601 Módulo K
Ed. Antônio Ernesto de Salvo
Brasília/DF - CEP 70.830-021
Telefone: (61) 2109-1400

	Possuir cabo de alimentação para a fonte com, no mínimo, 1,80m (um metro e oitenta centímetros) de comprimento.
Administração e Gerenciamento	Deverá ser configurável e gerenciável via GUI (graphical user interface) e CLI (command line interface); Deverá ser fornecido cabo de console compatível com a porta de console do equipamento; Implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps; Deverá possuir suporte a MIB II, conforme RFC 1213; Deverá possuir armazenamento interno das mensagens de log geradas pelo equipamento de no mínimo 2.048 bytes ou capacidade de armazenar no mínimo 1.000 mensagens; Implementar nativamente 4 (quatro) grupos RMON; Possibilitar a obtenção via SNMP de informações de capacidade e desempenho da CPU, memória e portas; Implementar os protocolos LLDP (IEEE 802.1AB) e LLDP-MED; Permitir a gravação de log externo em servidor Syslog; Implementar Telnet; Implementar Secure Shell (SSHv2); Implementar NTP ou SNTP; Implementar DHCP Client; Permitir o armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior à queda de alimentação.
VLAN	Implementar VLANs compatíveis com o padrão IEEE 802.1q; Implementar VLANs por porta; Implementar mecanismo de seleção de quais VLANs serão permitidas através de trunk 802.1q. Deverá ser permitida a configuração dessa seleção de forma dinâmica; Permitir a criação, remoção, gerenciamento e distribuição de VLANs de forma dinâmica através de portas configuradas como tronco IEEE 802.1Q; Permitir a criação de subgrupos dentro de uma mesma VLAN com conceito de portas isoladas e portas compartilhadas ("promíscuas"), onde portas isoladas não se comunicam com outras portas isoladas, mas apenas com as portas compartilhadas ("promíscuas") de uma dada VLAN.
Padrões	Implementar o padrão IEEE 802.1d; Implementar o padrão IEEE 802.1q; Implementar o padrão IEEE 802.1p; Implementar o padrão IEEE 802.3ad; Implementar o padrão IEEE 802.3af; Implementar o padrão IEEE 802.
Multicast	Implementar em todas as interfaces do switch o protocolo IGMP Snooping (v1, v2 e v3), não permitindo que o tráfego multicast seja tratado como broadcast no switch;
Qualidade de Serviço (QoS)	Possuir a facilidade de priorização de tráfego através do protocolo IEEE 802.1p; Suportar funcionalidades de QoS de "Traffic Shaping" e "Traffic Policing"; Deverá ser possível especificar a banda por classe de serviço; Suportar diferenciação de QoS por VLAN.

Serviço Nacional de Aprendizagem Rural

www.senar.org.br

SGAN Quadra 601 Módulo K
Ed. Antônio Ernesto de Salvo
Brasília/DF - CEP 70.830-021
Telefone: (61) 2109-1400

Garantia e Níveis de Serviço (SLA)	
Período	Os equipamentos deverão ser fornecidos com garantia do fabricante, suporte técnico do fabricante e todas as atualizações de software e assinaturas das funcionalidades requeridas neste Termo de Referência. A garantia do equipamento deverá ser on-site e de no mínimo 36 meses.
Atendimento	O atendimento deverá ser no regime de 7x24 a ser realizado diretamente pelo fabricante do equipamento ou pela contratada, caso o fabricante a tenha certificado para tal.
Cobertura	A garantia deverá cobrir todos os itens que compõem o equipamento.
Chamado	A abertura de chamados deverá ser realizada através de chamada telefônica, para número fixo, em regime de 24x7. Opcionalmente, os chamados poderão ser abertos através do site na internet.

LOTE II – EQUIPAMENTOS DE REDE	
ITEM 2 – SWITCHES 24 PORTAS	
QUANTIDADE	**12**
AQUISIÇÃO IMEDIATA: 04 EM TANGARÁ DA SERRA/MT	**04**
Características Gerais	Deverá possuir, no mínimo, 24 (vinte e quatro) portas ethernet 10/100/1000BASE-T com autosensing de velocidade, conectores RJ-45; Possuir, adicionalmente às portas especificadas no item anterior, no mínimo, 4 (quatro) slots SFP LAN Base; As interfaces 10/100/1000BASE-T deverão obedecer às normas técnicas IEEE802.3 (10BASE-T), IEEE802.3u (100BASE-TX), 802.3ab (1000BASE-T) e IEEE802.3x (Flow Control); Todas as portas Ethernet 10/100/1000BASE-T deverão suportar autoconfiguração de crossover (Auto MDIX); Todas as portas Ethernet 10/100/1000BASE-T deverão suportar configuração Half-Duplex e Full-Duplex, com a opção de negociação automática; Suportar Jumbo frames de no mínimo 9.216 bytes; Permitir montagem em rack padrão de 19 (dezenove) polegadas, possuindo, no máximo, 1 RU (uma unidade de rack) de altura. Deverão ser ofertados os acessórios necessários para a correta instalação; Possuir LEDs para a indicação do status e atividade das portas, além, do modo de operação full-duplex ou half-duplex; Deverá ser fornecido com documentação técnica e manuais que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização do equipamento.
Fonte de Alimentação	Possuir fonte de alimentação AC bivolt, com seleção automática de tensão (na faixa de 100 a 240V) e frequência de 50/60 Hz; Suportar alimentação elétrica capaz de suportar o equipamento com todas as funcionalidades especificadas; Possuir cabo de alimentação para a fonte com, no mínimo, 1,80m (um metro e oitenta centímetros) de comprimento.
Administração e Gerenciamento	Deverá ser configurável e gerenciável via GUI (graphical user interface) e CLI (command line interface); Deverá ser fornecido cabo de console compatível com a porta de console do equipamento;

Serviço Nacional de Aprendizagem Rural

www.senar.org.br

SGAN Quadra 601 Módulo K
Ed. Antônio Ernesto de Salvo
Brasília/DF - CEP 70.830-021
Telefone: (61) 2109-1400

	Implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps; Deverá possuir suporte a MIB II, conforme RFC 1213; Deverá possuir armazenamento interno das mensagens de log geradas pelo equipamento de no mínimo 2.048 bytes ou capacidade de armazenar no mínimo 1.000 mensagens; Implementar nativamente 4 (quatro) grupos RMON; Possibilitar a obtenção via SNMP de informações de capacidade e desempenho da CPU, memória e portas; Implementar os protocolos LLDP (IEEE 802.1AB) e LLDP-MED; Permitir a gravação de log externo em servidor Syslog; Implementar Telnet; Implementar Secure Shell (SSHv2); Implementar NTP ou SNTP; Implementar DHCP Client; Permitir o armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior à queda de alimentação.
VLAN	Implementar VLANs compatíveis com o padrão IEEE 802.1q; Implementar VLANs por porta; Implementar mecanismo de seleção de quais VLANs serão permitidas através de trunk 802.1q. Deverá ser permitida a configuração dessa seleção de forma dinâmica; Permitir a criação, remoção, gerenciamento e distribuição de VLANs de forma dinâmica através de portas configuradas como tronco IEEE 802.1Q; Permitir a criação de subgrupos dentro de uma mesma VLAN com conceito de portas isoladas e portas compartilhadas ("promíscuas"), onde portas isoladas não se comunicam com outras portas isoladas, mas apenas com as portas compartilhadas ("promíscuas") de uma dada VLAN.
Padrões	Implementar o padrão IEEE 802.1d; Implementar o padrão IEEE 802.1q; Implementar o padrão IEEE 802.1p; Implementar o padrão IEEE 802.3ad; Implementar o padrão IEEE 802.3af; Implementar o padrão IEEE 802.
Multicast	Implementar em todas as interfaces do switch o protocolo IGMP Snooping (v1, v2 e v3), não permitindo que o tráfego multicast seja tratado como broadcast no switch;
Qualidade de Serviço (QoS)	Possuir a facilidade de priorização de tráfego através do protocolo IEEE 802.1p; Suportar funcionalidades de QoS de "Traffic Shaping" e "Traffic Policing"; Deverá ser possível especificar a banda por classe de serviço; Suportar diferenciação de QoS por VLAN.
Garantia e Níveis de Serviço (SLA)	
Período	Os equipamentos deverão ser fornecidos com garantia do fabricante, suporte técnico do fabricante e todas as atualizações de software e assinaturas das funcionalidades requeridas neste Termo de Referência. A garantia do equipamento deverá ser on-site e de no mínimo 36 meses.

Serviço Nacional de Aprendizagem Rural

www.senar.org.br

SGAN Quadra 601 Módulo K
Ed. Antônio Ernesto de Salvo
Brasília/DF - CEP 70.830-021
Telefone: (61) 2109-1400

Atendimento	O atendimento deverá ser no regime de 7x24 a ser realizado diretamente pelo fabricante do equipamento ou pela contratada, caso o fabricante a tenha certificado para tal.
Cobertura	A garantia deverá cobrir todos os itens que compõem o equipamento.
Chamado	A abertura de chamados deverá ser realizada através de chamada telefônica, para número fixo, em regime de 24x7. Opcionalmente, os chamados poderão ser abertos através do site na internet.

LOTE III – EQUIPAMENTOS E SOFTWARE	
ITEM 1 – APPLIANCE DE FIREWALL COM GERENCIAMENTO UNIFICADO DE AMEAÇAS (UTM)	
QUANTIDADE	**06**
AQUISIÇÃO IMEDIATA: 02 EM TANGARÁ DA SERRA/MT	**02**
Requisitos Gerais	Aquisição de solução de Firewall para proteção de informação perimetral e de rede interna que inclui stateful firewall com capacidade para operar em alta disponibilidade (HA) em modo ativo-passivo ou ativo-ativo para controle de tráfego de dados por identificação de usuários e por camada 7, com controle de aplicação, administração de largura de banda (QoS), VPN IPsec e SSL, IPS, prevenção contra ameaças de vírus, malwares, filtro de URL, proteção de email, inspeção de tráfego criptografado e proteção de firewall de aplicação Web. Deverá ser fornecida console de gerenciamento dos equipamentos e centralização de logs em nuvem localizada no brasil visando garantir a conformidade com as legislações locais de proteção de dados e proporcionar melhor desempenho e menor latência. A console de gerenciamento deve ser possível atribuir configurações de concentradores de SD-WAN e dispor de configurações globais para replicação nos firewalls; Por cada appliance físico que compõe a plataforma de segurança, entende-se o hardware, software e as licenças necessárias para o seu funcionamento. Os equipamentos de firewall deverão ser novos, de primeiro uso, do último modelo disponível e em linha de fabricação. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico. Deve possuir processadores próprios e para fins específicos, desenvolvidos exclusivamente pelo fabricante da solução, com a finalidade de processar tráfegos de redes e acelerar o processamento destes pacotes de redes, permitindo o uso de diversas funcionalidades de segurança ao mesmo tempo sem diminuir a performance do equipamento. Todos os equipamentos de rede deverão possuir certificado de homologação expedido pela Agência Nacional de Telecomunicações (ANATEL). A solução deverá contemplar a totalidade das capacidades exigidas, sendo permitido o uso de mais de um equipamento (sempre em modo de alta disponibilidade HA) para complementar a solução, caso o fabricante não possua todas as funções em um único equipamento. Cada appliance deverá ser capaz de executar a totalidade das capacidades exigidas para cada função, não sendo aceitos somatórias para atingir os limites mínimos. O hardware e o software fornecidos não podem constar, no momento da apresentação da proposta, em listas de end-of-sale, end-of-support, end-of-engineering-support ou end-of-life do fabricante, ou seja, não poderão ter previsão

Serviço Nacional de Aprendizagem Rural

www.senar.org.br

SGAN Quadra 601 Módulo K
Ed. Antônio Ernesto de Salvo
Brasília/DF - CEP 70.830-021
Telefone: (61) 2109-1400

	de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante.
Características do Hardware	Interfaces Ethernet (fixas) 8 X GbE copper e 2 X SFP fibra Portas de Gerenciamento: 1 X RJ45 MGMT 1 X COM RJ45 1 X Micro-USB (Cabo incluso) Armazenamento (local quarantine/logs) 120 GB SATA-III SSD integrado Portas de E/S 2 x USB 3.0 (frontal) 1 x USB 2.0 (traseira) 1 X Slot porta flexível Display Módulo LCD multifuncional Fonte de alimentação faixa automática interna 100-240 VCA, 50-60 Hz Firewall throughput 30.00 Mbps Firewall IMIX 15.900 Mbps IPS throughput 5.800 Mbps Threat Protection throughput 1.250 Mbps Conexões simultâneas 6.500,000 Novas conexões/segundo 134.700 IPsec VPN throughput 3.000 Mbps SSL/TLS inspection 1.100 Mbps SSL conexões simultâneas 18.432
Firewall	A solução deve consistir em appliance de proteção de rede com funcionalidades de Next Generation Firewall (NGFW), e console de gerência, monitoração e logs. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7. O software deverá ser fornecido em sua versão mais atualizada. O HA (modo de alta disponibilidade) deve suportar o uso de dois equipamentos em modo ativo-passivo ou modo ativo-ativo e deve possibilitar monitoração de falha de link. Uma interface completa de comando de linha (CLI command-line-interface) deverá ser acessível através da interface gráfica e via porta serial. A atualização de software deverá enviar avisos de atualização automáticos. O sistema de objetos deverá permitir a definição de redes, serviços, hosts períodos de tempos, usuários e grupos, clientes e servidores. Os backups deverão ser feitos e armazenados localmente, via FTP e email com frequência diária, semanal ou mensal, podendo também ser realizado por demanda. As notificações deverão ser realizadas via email e SNMP. Suportar SNMPv3 e Netflow. O firewall deverá ser stateful, com inspeção profunda de pacotes.

Serviço Nacional de Aprendizagem Rural

www.senar.org.br

SGAN Quadra 601 Módulo K
Ed. Antônio Ernesto de Salvo
Brasília/DF - CEP 70.830-021
Telefone: (61) 2109-1400

	As zonas deverão ser divididas pelo menos em WAN, LAN e DMZ, sendo necessário que as zonas LAN e DMZ possam ser customizáveis. As políticas de NAT deverão ser customizáveis para cada regra. A proteção contra flood deverá ter proteção contra DoS (Denial of Service), DdoS (Distributed DoS). Proteção contra anti-spoofing. Suportar IPv4 e IPv6. Possuir certificação IPv6 Ready; IPv6 deve suportar os tunelamentos 6in4, 6to4, 4in6 e IPv6 Rapid Deployment (6rd) de acordo com a RFC 5969. Suporte aos roteamentos estáticos, dinâmico (RIP, BGP e OSPF, OSPFv3) e multicast (PIM-SM e IGMP). Deve suportar Roteamento BGP com uso de IPv6; Suportar Delegação de Prefixo IPV6 (DHCP PD); O firewall deve possuir integração com a plataforma de ZTNA do mesmo fabricante ou integração de terceiros; Deve possuir tecnologia de conectividade SD-WAN; A funcionalidade SD-WAN deve suportar conectividade com o Secure SD-WAN oferecido no serviço Microsoft Azure Virtual WAN; Deve suportar perfis de SD-WAN para balancear a carga das conexões entre as interfaces, Deve possuir métodos de balanceamento: round-robin e persistência de sessão com as seguintes opções: conexão: IP de origem; IP de destino; IP de origem e destino. Os links podem ser ponderados para determinar como o tráfego é distribuído entre eles, podendo usar o SLA para selecionar quais links serão incluídos no balanceamento de carga. Deve suportar a configuração de nível mínimo de qualidade (latência, jitter e perda de pacotes) para que determinado link seja escolhido pelo SDWAN; Deve suportar o uso de, no mínimo, 3 (três) links; Deve suportar o uso de links de interfaces físicas, sub-interfaces lógicas de VLAN e túneis IPSec; Deve gerar log de eventos que registrem alterações no estado dos links do SD-WAN, monitorados pela checagem de saúde; A solução deverá ser capaz de medir o status de saúde do link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss, onde seja possível configurar um valor de Theshold para cada um destes itens, onde será utilizado como fator de decisão nas regras de SD-WAN; A solução de SD-WAN deve ser capaz de apresentar de forma gráfica, todos os dados de análise da saúde dos links, contendo gráficos que apresentam no mínimo os critérios descritos acima; A checagem de estado de saúde deve suportar a marcação de pacotes com DSCP, para avaliação mais precisa de links que possuem QoS configurado A solução deve possuir funcionalidade de criação da malha SD-WAN em diversos firewalls em um único concentrador; Esta funcionalidade deve facilitar a configuração do SD-WAN de múltiplos firewalls, criando automaticamente todas as informações necessárias para que o SD-WAN

Serviço Nacional de Aprendizagem Rural

www.senar.org.br

SGAN Quadra 601 Módulo K
Ed. Antônio Ernesto de Salvo
Brasília/DF - CEP 70.830-021
Telefone: (61) 2109-1400

	aconteça, como pelo menos, mas não se limitando a: criação de rotas, regras de firewall, objetos e túneis VPNs necessárias; A mesma console do concentrador de SD-WAN deve monitorar os links de cada dispositivo implementado, garantindo uma visualização única de todos os dispositivos implementados; Deve possibilitar o roteamento baseado em VPNs; Deve suportar criar políticas de roteamento; Para as políticas de roteamento, devem ser permitidas pelo menos as seguintes condições: Interface de entrada do pacote; IPs de origem; IPs de destino; Portas de destino; Usuários ou grupos de usuários; Aplicação em camada 7 Deve ser possível escolher um gateway primário e um gateway de backup para as políticas de roteamento Deve suportar a definição de VLANs no firewall conforme padrão IEEE 802.1q e tagging de VLAN. Deve suportar Extended VLAN; O balanceamento de link WAN deve permitir múltiplas conexões de links Internet, checagem automática do estado de links, failover automático e balanceamento por peso. A solução deverá permitir port-aggregation de interfaces de firewall suportando o protocolo 802.3ad, para escolhas entre aumento de throughput e alta disponibilidade de interfaces; Deve permitir a configuração de jumbo frames nas interfaces de rede; Deve permitir a criação de um grupo de portas layer2; A Solução física deverá apresentar compatibilidade com modens USB (3G/4G), onde apenas seja acionado na eventualidade de falha no link principal; A solução deverá permitir configurar os serviços de DNS, Dynamic DNS, DHCP e NTP; O traffic shapping (QoS) deverá ser baseado em rede ou usuário. A solução deve permitir o tráfego de cotas baseados por usuários para upload/download e pelo tráfego total, sendo cíclicas ou não-cíclicas. Deve possuir otimização em tempo real de voz sobre IP. Deve implementar o protocolo de negociação Link Aggregation Control Protocol (LACP).
Prevenção de Ameaças	Deve realizar a inspeção profunda de pacotes para prevenção de intrusão (IPS) e deve incluir assinaturas de prevenção de intrusão (IPS). As assinaturas de prevenção de intrusão (IPS) devem ser customizadas. Exceções por usuário, grupo de usuários, IP de origem ou de destino devem ser possíveis nas regras; Deve suportar granularidade nas políticas de IPS Antivírus e Anti-Malware, possibilitando a criação de diferentes políticas por endereço de origem, endereço de destino, serviço e a combinação de todos esses itens, com customização completa; A solução contratada deve realizar a emulação de malwares desconhecidos em ambientes de sandbox em nuvem;

Serviço Nacional de Aprendizagem Rural

www.senar.org.br

SGAN Quadra 601 Módulo K
Ed. Antônio Ernesto de Salvo
Brasília/DF - CEP 70.830-021
Telefone: (61) 2109-1400

	Para a eficácia da análise de malwares Zero-Day, a solução de Sandbox deve possuir algoritmos de inteligência artificial, como algoritmos baseados em machine learning ; A funcionalidade de sandbox deve atuar como uma camada adicional ao motor de antimalware, e ao fim da análise do artefato, deverá gerar um relatório contendo o resultado da análise, bem como os screenshots das telas dos sistemas emulados pela plataforma; Deve permitir configuração da exclusão de tipos de arquivos para que não sejam enviados para o sandbox em nuvem; A proteção Anti-Malware deverá bloquear todas as formas de vírus, web malwares, trojans e spyware em HTTP e HTTPS, FTP e web-emails. A proteção Anti-Malware deverá realizar a proteção com emulação JavaScript. Deve ter proteção em tempo real contra novas ameaças criadas. Deve possuir pelo menos duas engines de anti-vírus independentes e de diferentes fabricantes para a detecção de malware, podendo ser configuradas isoladamente ou simultaneamente. Deve permitir o bloqueio de vulnerabilidades. Deve permitir o bloqueio de exploits conhecidos. Deve detectar e bloquear o tráfego de rede que busque acesso a command and control e servidores de controle utilizando múltiplas camadas de DNS, AFC e firewall. Deve incluir proteção contra ataques de negação de serviços. Ser imune e capaz de impedir ataques básicos como: SYN flood, ICMP flood, UDP Flood, etc. Suportar bloqueio de arquivos por tipo. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo. Os eventos devem identificar o país de onde partiu a ameaça. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas de segurança considerando uma das opções ou a combinação de todas elas: usuários, grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por usuários, grupos de usuários, origem, destino, zonas de segurança. O appliance deve ter a capacidade de atuar como um gateway antispam de modo que possa realizar filtragens dos emails e aplicar políticas. O gateway de email incluso no apliance deve ter pelo menos as seguintes proteções: Sender Policy Framework (SPF); Domain Keys Identified Mail (DKIM); Domain-based Message Authentication, Reporting & Conformance (DMARC); Bounce Address Tag Validation (BATV); O filtro de email deve quarentenar os emails suspeitos ou realmente maliciosos; A solução deve possibilitar aos usuários acessarem um painel para verificação da sua caixa pessoal de quarentena, possibilitando então a liberação ou a exclusão das mensagens; A função de antispam deve permitir a configuração de relays com a possibilidade de autenticação dos mesmos;

Serviço Nacional de Aprendizagem Rural

www.senar.org.br

SGAN Quadra 601 Módulo K
Ed. Antônio Ernesto de Salvo
Brasília/DF - CEP 70.830-021
Telefone: (61) 2109-1400

	A função de antispam deve possibilitar também o envio de emails seguros, realizando a criptografia das mensagens bem como dos seus anexos.
Políticas de Firewall	Deve suportar controles por: porta e protocolos TCP/UDP, origem/destino e identificação de usuários. As políticas deverão ter controle de tempo de acesso por usuário e grupo, sendo aplicadas por zonas, redes e por tipos de serviços. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança. Controle de políticas por países via localização por IP. Suporte a objetos e regras IPv6. Suporte a objetos e regras multicast.
Controle de Aplicações	Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações por assinaturas e camada 7, utilizando portas padrões (80 e 443), portas não padrões, port hopping e túnel através de tráfego SSL encriptado. Deve ser possível inspecionar os pacotes criptografados com os algoritmos SSL 2.0, SSL 3.0, TLS 1.2 e TLS 1.3. O motor de análise de tráfego criptografado deve reconhecer, mas não limitado a, pelo menos os seguintes algorítimos: curvas elipticas (ECDH, ECDHE, ECDSA), DH, DHE, Authentication, RSA, DSA, ANON, Bulk ciphers, RC4, 3DES, IDEA, AES128, AES256, Camellia, ChaCha20-Poly1305, GCM, CCM, CBC, MD5, SHA1, SHA256, SHA384. O motor de inspeção dos pacotes criptografados deve ser configurável e permitir definir ações como não decriptografar, negar o pacote e criptografar para determinadas conexões criptografadas Reconhecer pelo menos 2.300 aplicações diferentes, classificadas por nível de risco, características e tecnologia, incluindo, mas não limitado a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, serviços de rede, VoIP, streaming de mídia, proxy e tunelamento, mensageiros instantâneos, compartilhamento de arquivos, web e-mail e update de softwares. Reconhecer pelo menos as seguintes aplicações: 4Shared File Transfer, Active Directory/SMB, Citrix ICA, DHCP Protocol, Dropbox Download, Easy Proxy, Facebook Graph API, Firefox Update, Freegate Proxy, FreeVPN Proxy, Gmail Video, Chat Streaming, Gmail WebChat, Gmail WebMail, Gmail-Way2SMS WebMail, Gtalk Messenger, Gtalk Messenger File Transfer, Gtalk-Way2SMS, HTTP Tunnel Proxy, HTTPort Proxy, LogMeIn Remote Access, NTP, Oracle database, RAR File Download, Redtube Streaming, RPC over HTTP Proxy, Skydrive, Skype, Skype Services, skyZIP, SNMP Trap, TeamViewer Conferencing e File Transfer, TOR Proxy, Torrent Clients P2P, Ultrasurf Proxy, UltraVPN, VNC Remote Access, VNC Web Remote Access, WhatsApp, WhatsApp File Transfer e WhatsApp Web. Deve realizar o escaneamento e controle de micro app incluindo, mas não limitado a: Facebook (Applications, Chat, Commenting, Events, Games, Like Plugin, Message, Pics Download e Upload, Plugin, Post Attachment, Posting, Questions, Status Update, Video Chat, Video Playback, Video Upload, Website), Freegate Proxy, Gmail (Android Application, Attachment), Google Drive (Base, File Download, File Upload), Google Earth Application, Google Plus, LinkedIN (Company Search, Compose Webmail, Job Search, Mail Inbox, Status Update), SkyDrive File Upload e Download, Twitter (Message, Status Update, Upload, Website), Yahoo (WebMail, WebMail File Attach) e Youtube (Video Search, Video Streaming, Upload, Website)

Serviço Nacional de Aprendizagem Rural

www.senar.org.br

SGAN Quadra 601 Módulo K
Ed. Antônio Ernesto de Salvo
Brasília/DF - CEP 70.830-021
Telefone: (61) 2109-1400

	Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante. Atualizar a base de assinaturas de aplicações automaticamente. Reconhecer aplicações em IPv6. Limitar a banda usada por aplicações (traffic shaping). Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory e Azure AD, sem a necessidade de instalação de agente. Deve ser possível adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras. Deve permitir o uso individual de diferentes aplicativos para usuários que pertencem ao mesmo grupo de usuários, sem que seja necessária a mudança de grupo ou a criação de um novo grupo. Os demais usuários deste mesmo grupo que não possuírem acesso a estes aplicativos devem ter a utilização bloqueada.
Controle e Proteção WEB	Deve permitir especificar política de navegação Web por tempo, ou seja, a definição de regras para um determinado dia da semana e horário de início e fim, permitindo a adição de múltiplos dias e horários na mesma definição de política por tempo. Esta regra de tempo pode ser recorrente ou em uma única vez. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs e redes; Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via LDAP, Active Directory, Azure AD, Radius, E-directory e base de dados local; Deve permitir autenticação em 2 fatores em conjunto com a autenticação Radius; Permitir popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório; Possuir pelo menos 90 categorias de URLs; Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL; Deve ser capaz de forçar o uso da opção Safe Search em sites de busca; Deve ser capaz de forçar as restrições do Youtube; Deve ser capaz de categorizar as URLs a partir de base ou cache de URLs locais ou através de consultas dinâmicas na nuvem do fabricante, independentemente do método de classificação a categorização não deve causar atraso na comunicação visível ao usuário; Suportar a criação categorias de URLs customizadas; Suportar a opção de bloqueio de categoria HTTP e liberação da categoria apenas em HTTPS. Deve ser possível reconhecer o pacote HTTP independentemente de qual porta esteja sendo utilizada Suportar a inclusão nos logs do produto de informações das atividades dos usuários; Deve salvar nos logs as informações adequadas para geração de relatórios indicando usuário, tempo de acesso, bytes trafegados e site acessado. Deve permitir realizar análise flow dos pacotes, entendendo exatamente o que aconteceu com o pacote em cada checagem; Deve ser possível realizar caching do conteúdo web;

Serviço Nacional de Aprendizagem Rural

www.senar.org.br

SGAN Quadra 601 Módulo K
Ed. Antônio Ernesto de Salvo
Brasília/DF - CEP 70.830-021
Telefone: (61) 2109-1400

	Deve realizar filtragem por mime-type, extensão e tipos de conteúdo ativos, tais como, mas não limitado a: ActiveX, applets e cookies. Deve ser possível realizar a liberação de cotas de navegação para os usuários, permitindo que os usuários tenham tempos pré-determinados para acessar sites na internet. A console de gerenciamento deve possibilitar a visualização do tempo restante para cada usuário, bem como reiniciar o tempo restante com o intuito de zerar o contador. Deve possuir capacidade de alguns usuários previamente selecionados realizarem um bypass temporário na política de bloqueio atual. A solução deve permitir o enforce dos domínios do Google e Office365 a fim de determinar em quais domínios os usuários poderão se autenticar.
Controle e identificação de usuários	Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticando via LDAP, Active Directory, Azure AD, Radius, eDirectory, TACACS+ e via base de dados local, para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços. Deve permitir autenticação em modos: transparente, autenticação proxy (explicito, NTLM e Kerberos) e autenticação via clientes nas estações com os sistemas operacionais Windows, macOS e Linux 32/64. Ao se utilizar da opção de proxy explicito, deve permitir a autenticação por cada conexão, a fim de garantir que usuários logados em servidores de multisessão sejam identificados corretamente pelo firewall, mesmo quando utilizando-se apenas 1 IP de origem; Deve possuir a autenticação Single sign-on para, pelo menos, os sistemas de diretórios Active Directory, Azure AD e eDirectory; Dever suportar a configuração de logon único (Single sign-on) para que os administradores façam logon no console da Web usando o Azure AD; Deve possuir portal do usuário para que os usuários tenham acesso ao uso de internet pessoal, troquem senhas da base local e façam o download de softwares para as estações presentes na solução.
Qualidade do Serviço (QOS)	Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações. A solução deverá suportar Traffic Shaping (Qos) e a criação de políticas baseadas em categoria web e aplicação por: endereço de origem; endereço de destino; usuário e grupo do LDAP/AD. Deve ser configurado o limite e a garantia de upload/download, bem como ser priorizado o tráfego total e bitrate de modo individual ou compartilhado. Suportar priorização Real-Time de protocolos de voz (VoIP). Deve permitir aplicar prioridade mesmo após o roteamento, utilizando o protocolo DSCP.

Serviço Nacional de Aprendizagem Rural

www.senar.org.br

SGAN Quadra 601 Módulo K
Ed. Antônio Ernesto de Salvo
Brasília/DF - CEP 70.830-021
Telefone: (61) 2109-1400

VPN	Suportar VPN Site-to-Site e Cliente-to-Site. Suportar IPsec VPN. Suportar SSL VPN. Suportar L2TP e PPTP. Suportar acesso remoto SSL, IPSec e VPN Client para Android e iPhone/iPAD. Deve ser disponibilizado o acesso remoto ilimitado, até o limite suportado de túneis VPN pelo equipamento, sem a necessidade de aquisição de novas licenças e sem qualquer custo adicional para o licenciamento de clientes SSL. Deve possuir o acesso via o portal de usuário para o download e configuração do cliente SSL para Windows. Deve possuir opção de VPN IPSEC com client nativo do fabricante. Deve possuir um portal encriptado baseado em HTML5 para suporte pelo menos a: RDP, SSH, Telnet e VNC, sem a necessidade de instalação de clientes VPN nas estações de acesso. A VPN IPsec deve suportar: DES, 3DES, GCM, Suite-B, Autenticação MD5 e SHA-1;Diffie-Hellman Group 1, Group 2, Group 5 e Group 14; Algoritmo Internet Key Exchange (IKE); AES 128, 192 e 256 (Advanced Encryption Standard); SHA 256, 384 e 512; Autenticação via certificado PKI (X.509) e Pre-shared key (PSK). Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, SonicWALL, Fortinet, Huawei, Juniper, Palo Alto Networks e Sophos. Deve suportar nativamente a integração com a Amazon, a fim de estabelecer um túnel seguro entre os appliances e o conentrador VPN da AWS. Deve permitir criar políticas de controle de aplicações, IPS, Antivírus, Anti-Malware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL; Suportar autenticação via AD/LDAP, Token e base de usuários local; Permitir estabelecer um túnel SSL VPN com uma solução de autenticação via LDAP, Active Directory, Azure AD, Radius, eDirectory, TACACS+ e via base de dados local.
Gerenciamento	Deve possuir solução de gerenciamento centralizado, possibilitando o gerenciamento de diversos equipamentos através de uma única console central, com administração de privilégios e funções. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança. Estar licenciada para gerenciar as soluções de firewall de próxima geração. Devem ser fornecidas soluções virtuais ou via appliances desde que obedeçam a todos os requisitos desta especificação. Deve ser centralizada a gerência de todas as políticas do firewall e configurações para as soluções de firewall, sem necessidade de acesso direto aos equipamentos. Deve permitir a criação de Templates para configurações. Deve possuir indicadores do estado de equipamentos e rede. Deve emitir alertas baseados em thresholds customizáveis, incluindo também alertas de expiração de subscrição, mudança de status de gateways, uso excessivo de disco, eventos ATP, IPS, ameaças de vírus, navegação, entre outros. Deve permitir a criação de grupos de equipamentos por nome, modelo, firmware e regiões. Deve ter controle de privilégios administrativos, com granularidade de funções (VPN admin, App e Web admin, IPS admin, etc); Deve ter controle das alterações feitas por usuários administrativos, comparar diferentes versões de configurações e realizar o processo de roll back de configurações para mudanças indesejadas;

Serviço Nacional de Aprendizagem Rural

www.senar.org.br

SGAN Quadra 601 Módulo K
Ed. Antônio Ernesto de Salvo
Brasília/DF - CEP 70.830-021
Telefone: (61) 2109-1400

	Deve ter logs de auditoria de uso administrativo e atividades realizadas nos equipamentos. Deve ter integração com a solução de logs e relatórios, habilitando o provisionamento automático de novos equipamentos e a sincronização dos administradores da centralização da gerência com a centralização de logs e relatórios. Deve possibilitar o envio dos logs via syslog com conexão segura (TLS).
Serviço de Instalação	Os serviços de implantação deverão ter duração máxima de 15 dias corridos após o início de sua execução; Deverá incluir a instalação física dos equipamentos, incluindo as conexões lógicas e elétricas; Instalação, configuração e customização da solução; Instalação e configuração do ambiente de gerenciamento; Documentação do ambiente.
Treinamento	Treinamento hands-on a ser realizado no local da instalação ou virtual, sem quaisquer ÔNUS para a instituição, para o mínimo de 2 (duas) pessoas após a instalação completa do ambiente, contemplando obrigatoriamente os seguintes tópicos: a. Gerenciamento remoto de todos os recursos de hardware fornecidos; b. Uso das ferramentas de gerenciamento, administração, configuração e monitoração do produto, além de descrever os principais componentes do mesmo. c. O treinamento deverá possuir no mínimo 8 horas de duração.
Garantia e Níveis de Serviço (SLA)	
Período	Os equipamentos deverão ser fornecidos com garantia do fabricante, suporte técnico do fabricante e todas as atualizações de software e assinaturas das funcionalidades requeridas neste Termo de Referência. A garantia do equipamento deverá ser on-site e de no mínimo 36 meses.
Atendimento	O atendimento deverá ser no regime de 24x7, diretamente pelo fabricante do equipamento ou pela contratada, caso o fabricante a tenha certificado para tal.
Cobertura	A garantia deverá cobrir todos os itens que compõem o equipamento.
Chamado	A abertura de chamados deverá correr através de chamada telefônica para o número fixo, e-mail ou site para abertura de chamados no regime de 24x7.

LOTE III – EQUIPAMENTOS E SOFTWARE	
ITEM 2 – SOLUÇÃO DE WIRELESS COMPOSTA DE GERENCIAMENTO CENTRALIZADO, PONTOS DE ACESSO, INJETOR DE ENERGIA E GESTÃO DE CONEXÕES.	
QUANTIDADE	**39**
AQUISIÇÃO IMEDIATA: 13 EM TANGARÁ DA SERRA/MT	**13**

Serviço Nacional de Aprendizagem Rural

www.senar.org.br

SGAN Quadra 601 Módulo K
Ed. Antônio Ernesto de Salvo
Brasília/DF - CEP 70.830-021
Telefone: (61) 2109-1400

Requisitos Gerais	Fornecimento de equipamentos de rede wireless, contemplando controladora, pontos de acesso sem fio, licenças de uso e fontes de energia. Todos os produtos ofertados deverão pertencer à linha atual de produção dos fabricantes;
Características Específicas de Desempenho e Hardware Controladora Wireless	Deverá ser gerenciado de forma centralizada pelo Software de Gerência do mesmo fabricante do Access Point Sem Fio, para a configuração dos seus parâmetros Wi-Fi, QoS, políticas de acesso, políticas de segurança, monitoração do espectro de rádio frequência e demais funcionalidades, com conexão lógica via roteamento da camada de rede do modelo OSI, através de rede privada e pública; Deve permitir ser gerenciado através de interface GUI local, através de um browser; Deverá ser autoconfigurável através do Software de Gerência sem a necessidade de intervenção técnica para a sua configuração inicial (Zero Touch); Deverá atualizar a sua versão de firmware através do Software de Gerência; Deverá carregar e salvar as suas configurações através do Software de Gerência; Caso a comunicação entre o Access Point (AP) e o Software de Gerência seja interrompida, o AP deve continuar operando, permitindo que os dispositivos e usuários já autenticados e associados à rede sem fio continuem acessíveis e que novos clientes possam obter acesso; Todo o tráfego de/para os dispositivos cliente deve ser encaminhado localmente e em hipótese alguma ser direcionado para o Software de Gerência em Nuvem; Todo o tráfego de configuração, monitoria, gerência e estatísticas entre o Access Point e o Software de Gerência deverá ocorrer com a utilização de criptografia; Suportar a pilha de protocolos TCP/IP; Suportar os protocolos IPv4 e IPv6 simultaneamente; Implementar VLAN Tagging IEEE 802.1q; Implementar, localmente ou via software de gerência, o protocolo NTP ou SNTP no modo cliente para a sincronização de horário; Possuir cliente DHCP para a configuração automática dos seus parâmetros IP; Permitir alimentação elétrica no padrão IEEE 802.3at Plus (PoE+), utilizando a porta do switch PoE+ onde estiver conectado; Quando alimentado pela interface de rede via PoE+, não deve sofrer nenhuma perda de funcionalidade e operar no seu desempenho máximo; Não possuir restrição de licenças para a quantidade de dispositivos conectados simultaneamente; Implementar os padrões de segurança WPA2 Personal/Enterprise, WPA3 Personal, WPA3 Enterprise, OWE e Advanced Encryption Standard (AES); Permitir habilitar e desabilitar a divulgação de cada SSID de forma independente; Implementar Wireless Isolation para evitar que um dispositivo conectado a um SSID acesse os dados de outros dispositivos conectados no mesmo SSID;

Serviço Nacional de Aprendizagem Rural

www.senar.org.br

SGAN Quadra 601 Módulo K
Ed. Antônio Ernesto de Salvo
Brasília/DF - CEP 70.830-021
Telefone: (61) 2109-1400

	Implementar filtros baseados em protocolos e em endereços MAC; Implementar o reuso de frequências (BSS coloring); Implementar Target Wake Time para os clientes 802.11ax compatíveis; Deve implementar OFDMA; Deve suportar as funcionalidades de RADIUS Accounting, SNMP, Wireless Multimedia (WMM), Spanning Tree Protocol (STP), Bridge para LAN, Bridge para VLAN, Airtme Fairness, detecção de interferência, Fast roaming (802.11r), Band Steering, Autenticação via login social, Syslog e LLDP-MED; Deve ser capaz de detectar Rogue SSID, Evil Twin SSID, BSSID Impersonate SSID, SSID Impersonate, Advanced Impersonate SSID e Adhoc SSID; Disponibilizar sistema de hotspot vouchers baseado em tempo e volume de dados; Deverá possuir acesso restrito por usuário e senha, com capacidade de criação de diferentes perfis de acesso onde seja possível determinar as funcionalidades atribuídas a cada perfil, existindo, no mínimo, um perfil com permissões de criação de usuários visitantes e um perfil com permissão para efetuar qualquer alteração; Possuir listagem de clientes Wireless, indicando SSID, endereço IP e endereço MAC; Listagem de APs e o status de cada Ponto de Acesso de forma individual, exibindo informações sobre o canal, grupo e endereço MAC; Autenticação por Portal Web, onde conectados à rede são redirecionados para um Portal Web onde deverão se autenticar e então receber as políticas de acesso.
Pontos de Acesso	Access Point Sem Fio Wi-Fi 6E, gerenciado por Plataforma de Gerência em Nuvem, para uso interno, sem antenas aparentes, que opere simultaneamente nas faixas de frequência de 2.4GHz, 5GHz e 6GHz, padrões 802.11b/g/n/a/ac/ax; Deve possuir, no mínimo, 1 porta ethernet 100M/1000M/2.5G Base-T em conector RJ45 com suporte a alimentação PoE compatível com o padrão 802.3at; Suporte a velocidades de no mínimo 2400 Mbps em 6GHz, 2400 Mbps em 5GHz e 575 Mbps em 2.4GHz; Cada rádio deverá possuir, no mínimo, 6 antenas internas omnidirecionais, 2x 2.4 GHz, 2x 5 GHz, 2x 6 GHz, com ganho de, no mínimo, 4.2 dBi para 2.4 GHz, 5.5 dBi para 5 GHz e 5.5 dBi para 6 GHz. Suporte a operação 2x2:2 MIMO; Suportar a utilização de canais de 20, 40, 80 e 160 MHz; Suportar, no mínimo, 8 (oito) SSIDs por rádio, com capacidade de configuração de VLAN e políticas de acesso independentes para cada SSID; Possuir LED para a indicação do status de funcionamento do equipamento; O equipamento deverá ser novo, sem uso anterior e não pode constar na situação de “solicitação de venda encerrada” (end of sale) ou “solicitação de pedido suspensa” (end of order) pelo fabricante no momento da proposta; Deverá ser fornecido com a mais recente versão de hardware disponível na data da aquisição; Deverá vir acompanhado de todos os acessórios para sua operacionalização, como cabos, softwares e manuais. Os manuais poderão

Serviço Nacional de Aprendizagem Rural

www.senar.org.br

SGAN Quadra 601 Módulo K
Ed. Antônio Ernesto de Salvo
Brasília/DF - CEP 70.830-021
Telefone: (61) 2109-1400

	ser disponibilizados no site do fabricante em língua portuguesa (Brasil) ou inglesa; Deverá possuir mecanismo de segurança física no padrão Kensington lock hard point ou similar; A estrutura física do equipamento deverá permitir fixação em teto e em parede; Deverá conter todas as ferragens necessárias para a sua fixação em teto e em parede; Deve suportar DFS; Suportar temperatura em modo de operação entre 0° to 40° C.
Injetor de Energia	Fornecer alimentação elétrica dos APs via interface de rede 10/100/1000, de acordo com o padrão PoE (Power over Ethernet Plus), mantendo todas as suas funcionalidades e capacidade, calculados para o desempenho máximo do AP, ou seja, todos os transmissores e receptores que compõem o AP; Os Pontos de Acesso não poderão sofrer nenhum tipo de perda, seja performance, transmissão ou qualquer funcionalidade quando alimentado por Power over Ethernet Plus (PoE) conforme o padrão 802.3af; Deverá possuir fonte de alimentação com seleção automática de tensão (100– 240 VAC); Deverá ser específico para ambiente interno; Deverá fornecer no mínimo 20W; Deverá ser acompanhado de cabo de energia necessário para sua operacionalização.
Treinamento	Treinamento hands-on a ser realizado no local da instalação ou em centro especializado do próprio fornecedor, sem quaisquer ÔNUS para a instituição, para o mínimo de 2 (duas) pessoas após a instalação completa do ambiente, contemplando obrigatoriamente os seguintes tópicos: ➢ Gerenciamento de todos os recursos fornecidos; ➢ Uso das ferramentas de gerenciamento, administração, configuração e monitoração do produto, além de descrever os principais componentes do mesmo; ➢ O treinamento deverá possuir no mínimo 8 horas de duração.
Serviço de Instalação	Levantamento de requisitos para a execução; Elaboração de documento contendo as informações sobre o ambiente atual, análise da topologia de rede e apresentação da metodologia de implantação através de projeto de migração; Os serviços de implantação deverão ter duração máxima de 15 dias corridos após o início de sua execução; Deverá incluir a instalação física dos equipamentos, incluindo as conexões lógicas e elétricas; Instalação, configuração e customização da solução. Instalação e configuração do ambiente de gerenciamento; Documentação do ambiente.
Garantia e Níveis de Serviço (SLA)	
Período	Os equipamentos deverão ser fornecidos com garantia do fabricante, suporte técnico do fabricante e todas as atualizações de software e

Serviço Nacional de Aprendizagem Rural

www.senar.org.br

SGAN Quadra 601 Módulo K
Ed. Antônio Ernesto de Salvo
Brasília/DF - CEP 70.830-021
Telefone: (61) 2109-1400

	assinaturas das funcionalidades requeridas neste Termo de Referência. A garantia do equipamento deverá ser on-site e de no mínimo 36 meses.
Atendimento	O atendimento deverá ser no regime de 24x7, a ser realizado diretamente pelo fabricante do equipamento ou pela contratada, caso o fabricante a tenha certificado para tal.
Cobertura	A garantia deverá cobrir todos os itens que compõem o equipamento.
Chamado	A abertura de chamados deverá ser realizada através de chamada telefônica para o número fixo, no regime de 24x7. Opcionalmente, os chamados poderão ser abertos através do site na Internet.

LOTE III – EQUIPAMENTOS E SOFTWARE	
ITEM 3 - SOLUÇÃO DE ANTIVÍRUS GERENCIÁVEL	
QUANTIDADE	**285**
AQUISIÇÃO IMEDIATA: 95 EM TANGARÁ DA SERRA/MT	**95**
Características gerais	Todos os componentes que fazem parte da solução, de segurança para servidores, estações de trabalho deverão ser fornecidas por um único fabricante. Não serão aceitas composições de produtos de fabricantes diferentes; A console de monitoração e configuração deverá ser feita através de uma central única, baseada em web e em nuvem, que deverá conter todas a fermentas para a monitoração e controle da proteção dos dispositivos; O fabricante da console baseada em nuvem deve garantir disponibilidade de 99,8% no mês para cada funcionalidade. A console de gerência em nuvem deve permitir configurar autenticação em múltiplos fatores. Permitir a configuração de perfis com permissões agrupadas que possam ser vinculados às contas de acesso à solução, para possibilitar a segregação de funções. A console deverá apresentar Dashboard com o resumo dos status de proteção dos computadores e usuários, bem como indicar os alertas de eventos de criticidades alta, média e informacional; Permitir ao administrador criar diferentes políticas de segurança e aplicá-las a diferentes grupos de máquinas de acordo com seus atributos. Deve possuir mecanismo de comunicação via API, para integração com outras soluções de segurança, como por exemplo SIEM; A console deve permitir a divisão dos computadores, dentro da estrutura de gerenciamento em grupos; Deve permitir sincronização com o Active Directory (AD) para gestão de usuários e grupos integrados às políticas de proteção. Deve possuir a possibilidade de aplicar regras diferenciadas baseado em grupos, usuários ou dispositivos; A instalação deve ser feita via cliente específico por download da gerência central e também via e-mail de configuração. O instalador deverá permitir a distribuição do cliente via Active Directory (AD) para múltiplas máquinas Deve ser possível a instalação dos agentes de forma manual ou remota, com suporte à distribuição do agente por ferramentas de terceiros, incluindo o System Center Configuration Manager (SCCM) da Microsoft.

Serviço Nacional de Aprendizagem Rural

www.senar.org.br

SGAN Quadra 601 Módulo K
Ed. Antônio Ernesto de Salvo
Brasília/DF - CEP 70.830-021
Telefone: (61) 2109-1400

	Deve ser possível configurar parâmetros de linha de comando para configurar pelo menos os seguintes itens: Instalação silenciosa; Proxy de rede; Nome do dispositivo; O agente deve ser classificado pelo Windows como solução de Antivírus (anti-malware). Deve ser possível armazenar os dados da instalação e transformar estes dados em um cache da instalação, de forma que possibilite a instalação em outros dispositivos utilizando-se deste cache com o intuito de reduzir o uso da largura de banda. Deve a console ser capaz de criar e editar diferentes políticas para a aplicação das proteções exigidas e aplicadas a nível de usuários, não importando em que equipamentos eles estejam acessando; Fornecer atualizações do produto e das definições de vírus e proteção contra intrusos; Deve permitir exclusões de escaneamento para um determinado website, arquivo, processos ou aplicação, tanto a nível geral quanto específico em uma determinada política. A console de gerenciamento deve permitir a definição de grupos de usuários com diferentes níveis de acesso as configurações, políticas e logs; Atualização incremental, remota e em tempo real, da vacina dos Antivírus e do mecanismo de verificação (Engine) dos clientes; A solução deve ter características de Endpoint, Detection and Response (EDR); O módulo de EDR deve ser gerenciado pela mesma console que o endpoint tradicional, não serão aceitas soluções que trabalham com mais de uma plataforma de gerenciamento; Pelo módulo de EDR, deve ser possível realizar buscas de itens suspeitos em todos os dispositivos que contenham a solução instalada; Estas buscas devem permitir pelo menos, mas não limitando-se a: Endereços de IP, Hashes, arquivos e linhas de comando; Deve exibir a reputação de um processo para uma análise da legitimidade do mesmo; Permitir o agendamento da varredura contra vírus com a possibilidade de selecionar uma máquina, grupo de máquinas ou domínio, com periodicidade definida pelo administrador; Atualização automática das assinaturas de ameaças (malwares) e políticas de prevenção desenvolvidas pelo fabricante em tempo real ou com periodicidade definida pelo administrador; Utilizar protocolos seguros padrão HTTPS para comunicação entre console de gerenciamento e clientes gerenciados. As mensagens geradas pelo agente deverão estar no idioma em Português ou permitir a sua edição. Permitir a exportação dos relatórios gerenciais para os formatos CSV e PDF; Recursos do relatório e monitoramento deverão ser nativos da própria console central de gerenciamento; Possibilidade de exibir informações como nome da máquina, versão do antivírus, sistema operacional, versão da engine, data da vacina, data da última verificação, eventos recentes e status;

Serviço Nacional de Aprendizagem Rural

www.senar.org.br

SGAN Quadra 601 Módulo K
Ed. Antônio Ernesto de Salvo
Brasília/DF - CEP 70.830-021
Telefone: (61) 2109-1400

	Permitir a configuração de alertas em tempo real de ameaças com envio de e-mail a usuários pré-definidos Capacidade de geração de relatórios, estatísticos ou gráficos, tais como: Detalhar quais usuários estão ativos, inativos ou desprotegidos, bem como detalhes dos mesmos; Detalhamento dos computadores que estão ativos, inativos ou desprotegidos, bem como detalhes das varreduras e dos alertas nos computadores; Detalhamento dos periféricos permitidos ou bloqueados, bem como detalhes de onde e quando cada periférico foi usado; Detalhamento das principais aplicações bloqueadas e os servidores/usuários que tentaram acessá-las; Detalhamento das aplicações permitidas que foram acessadas com maior frequência e os servidores/usuários que as acessam; Detalhamento dos servidores/usuários que tentaram acessar aplicações bloqueadas com maior frequência e as aplicações que eles tentaram acessar; Detalhamento de todas as atividades disparadas por regras de prevenção de perda de dados. A console de gerenciamento deve evidenciar de forma gráfica toda a rastreabilidade de um ataque, contendo toda a sequência de eventos que ocorreram durante a execução do malware, sendo possível ainda expandir os detalhes de cada informação e identificar informações como a causa raiz de um determinado ataque/infecção. Devem ser coletadas as atividades de todos artefatos analisados, contendo informações sobre interação com outros processos, arquivos e chaves de registro acessadas/modificadas, conexões de rede realizadas, dentre outras. Deve ser possível exportar essas informações. Permitir isolar a máquina, de maneira que ela perca a comunicação com a rede ou se comunique apenas com os servidores da solução ou com servidores e serviços definidos na política de isolamento. O agente deve ter a capacidade de fazer o isolamento da máquina por si só, sem precisar de nenhuma integração com outros softwares ou dispositivos de rede para isso. Deve ser possível ao administrador efetuar a liberação da máquina do isolamento via console de gerência ou fornecer uma chave para realizar a liberação. Deverá possuir um elemento de comunicação para mensagens e notificações entre estações e a console de gerenciamento utilizando comunicação criptografada. Deve fornecer solução de gerenciamento de arquivos armazenados em nuvem, garantindo que um arquivo que foi feito um upload (exemplo Dropbox), tenha o processo monitorado e gerenciado, bem como realizar automaticamente o escaneamento do arquivo contra malwares, procuradas palavras chaves ou informações confidenciais. A atualização da versão deverá ser transparente para os usuários finais. O agente antivírus deverá proteger laptops, desktops e servidores em tempo real, sob demanda ou agendado para detectar, bloquear e limpar todos os vírus, trojans, worms e spyware. No Windows o agente também deverá detectar PUA, adware, comportamento suspeito, controle de aplicações e

Serviço Nacional de Aprendizagem Rural

www.senar.org.br

SGAN Quadra 601 Módulo K
Ed. Antônio Ernesto de Salvo
Brasília/DF - CEP 70.830-021
Telefone: (61) 2109-1400

	dados sensíveis. O agente ainda deve fornecer controle de dispositivos terceiros e, controle de acesso à web; Deve possuir mecanismo contra a desinstalação do endpoint pelo usuário e cada dispositivo deverá ter uma senha única, não sendo autorizadas soluções com uma mesma senha válida para todos os dispositivos; Deve prover no endpoint a solução de HIPS (Host Instrusion Prevention System) para a detecção automática e proteção contra comportamentos maliciosos (análise de comportamento) e deverá ser atualizado automaticamente; Deve prover proteção automática contra web sites infectados e maliciosos, assim como prevenir o ataque de vulnerabilidades de browser via web exploits; Deve permitir a monitoração e o controle de dispositivos removíveis nos equipamentos dos usuários, como dispositivos USB, periféricos da própria estação de trabalho e redes sem fio, estando sempre atrelado ao usuário o controle e não ao dispositivo; O controle de dispositivos deve ser ao nível de permissão, como somente leitura ou bloqueio; Os seguintes dispositivos deverão ser, no mínimo, gerenciados: HD (hard disks) externos, pendrives USB, storages removíveis seguras, CD, DVD, Blu-ray, floppy drives, interfaces de rede sem fio, modems, bluetooth, infravermelho, MTP (Media Transfer Protocol) tais como Blackberry, iPhone e Android smartphone e PTP (Picture Transfer Protocol) como câmeras digitais; Deve possuir funcionalidades de monitoramento do firewall local do Windows A ferramenta de administração centralizada deverá gerenciar todos os componentes da proteção para estações de trabalho e servidores e deverão ser projetadas para a fácil administração, supervisão e elaboração de relatórios dos endpoint e servidores; Deverá possuir interface gráfica web, com suporte aos seguintes idiomas: Inglês (padrão); Português; Alemão; Francês; Italiano; Espanhol; Japonês; Chinês (tradicional e simplificado); A Console de administração deve incluir um painel com um resumo visual em tempo real para verificação do status de segurança; Deverá fornecer filtros pré-construídos que permitam visualizar e corrigir apenas os computadores que precisam de atenção; Deverá exibir os PCs gerenciados de acordo com critérios da categoria (detalhes do estado do computador, detalhes sobre a atualização, detalhes de avisos e erros, detalhes do antivírus, etc.), e classificar os PCs em conformidade; Uma vez que um problema seja identificado, deverá permitir corrigir os problemas remotamente, com no mínimo as opções abaixo: Proteger o dispositivo com a opção de início de uma varredura; Forçar uma atualização naquele momento; Ver os detalhes dos eventos ocorridos; Executar verificação completa do sistema; Forçar o cumprimento de uma nova política de segurança; Mover o computador para outro grupo; Apagar o computador da lista;

Serviço Nacional de Aprendizagem Rural

www.senar.org.br

SGAN Quadra 601 Módulo K
Ed. Antônio Ernesto de Salvo
Brasília/DF - CEP 70.830-021
Telefone: (61) 2109-1400

	Atualizar a políticas de segurança quando um computador for movido de um grupo para outro manualmente ou automaticamente; Gravar um log de auditoria seguro, que monitore a atividade na console de gerenciamento para o cumprimento de regulamentações, auditorias de segurança, análise e solução de problemas forenses; Deverá permitir exportar o relatório de logs de auditoria nos formatos CSV e PDF; Todos os logs devem ser armazenados pelo fabricante gratuitamente por pelo menos 90 dias. O agente deve ter a possibilidade de gerar um arquivo único contendo todos os logs e informações necessárias para que o suporte do fabricante possa realizar um troubleshooting avançado em casos de problemas. Deve conter vários relatórios para análise e controle dos usuários e endpoints. Os relatórios deverão ser divididos, no mínimo, em relatórios de: eventos, usuários, controle de aplicativos, periféricos e web, indicando todas as funções solicitadas para os endpoints; Fornecer relatórios utilizando listas ou gráficos, utilizando informações presentes na console, com no mínimo os seguintes tipos: Nome do dispositivo; Início da proteção; Ultimo usuário logado no dispositivo; Status do escaneamento em tempo real; Último update; Último escaneamento realizado; Status de proteção do dispositivo; Grupo a qual o dispositivo faz parte; Permitir a execução manual de todos estes relatórios, assim como o agendamento e envio automático por e-mail nos formatos CSV e PDF.
Características básicas do agente de proteção contra malwares	Pré-execução para verificar e detectar malwares desconhecidos, incluindo zero-days; O agente deve buscar algum sinal de malware ativo e detectar malwares desconhecidos; Deverá conter técnicas avançadas de detecção de malwares desconhecidos, utilizando algoritmos de inteligência artificial, como machine learning ou deep learning; Efetuar a análise baseada em técnicas de machine learning, inteligência artificial, anti-exploits ou threat intelligence, permitindo a proteção contra-ataques que explorem vulnerabilidades, mesmo que ainda não existam patches de correção O agente deve ter a capacidade de submeter o arquivo desconhecido à nuvem de inteligência do fabricante para detectar a presença de ameaças; O agente deve realizar a atualização várias vezes por dia para manter a detecção atualizada contra as ameaças mais recentes; A solução deve manter conexão direta com banco de dados de ameaças do fabricante para uso da rede de inteligência; Deve realizar a verificação de todos os arquivos acessados em tempo real; Deve realizar a verificação de todos os arquivos no disco rígido em intervalos programados; Deve realizar a limpeza do sistema automaticamente, removendo itens maliciosos detectados e aplicações potencialmente indesejáveis (PUA);

Serviço Nacional de Aprendizagem Rural

www.senar.org.br

SGAN Quadra 601 Módulo K
Ed. Antônio Ernesto de Salvo
Brasília/DF - CEP 70.830-021
Telefone: (61) 2109-1400

	Deve proteger os navegadores Internet Explorer, Firefox, Chrome, Opera e Safari, bloqueando o acesso a sites infectados conhecidos e pela verificação dos dados baixados antes de serem executados; Deve permitir a autorização de detecções maliciosas e excluir da varredura diretórios e arquivos específicos; É requerida a proteção integrada, ou seja, em um único agente, contra ameaças de segurança, incluindo vírus, spyware, trojans, worms, adware e aplicativos potencialmente indesejados (PUAs); Suportar máquinas com arquitetura 32-bit e 64-bit; O cliente para instalação em estações de trabalho deverá ser compatível com os sistemas operacionais, Mac OS X 10.10, 10.11, 10.12, Microsoft Windows Vista, 7, 8, 10; O cliente para instalação em estações de trabalho deverá ser compatível com os sistemas operacionais Linux CentOS 6/7, Mint 17, Ubuntu 14/16, Debian 7/8; Possuir a funcionalidade de proteção contra a alteração das configurações do agente, impedindo aos usuários, incluindo o administrador local, reconfigurar, desativar ou desinstalar componentes da solução de proteção; Permitir a utilização de senha de proteção para possibilitar a reconfiguração local no cliente ou desinstalação dos componentes de proteção.
Funcionalidade de Detecção e Proteção de Intrusão	Possuir proteção contra exploração de buffer overflow; Possuir proteção contra-ataques de Negação de Serviço (Denial of Service - DoS), Port-Scan, MAC Spoofing e IP Spoofing; Deverá possui atualização periódica de novas assinaturas de ataque; Capacidade de reconhecer e bloquear automaticamente as aplicações em clientes baseando-se na impressão digital (hash) do arquivo. Capacidade de bloqueio de ataques baseado na exploração de vulnerabilidade conhecidas; Possuir um sistema de prevenção de intrusão no host (HIPS), que monitore o código e blocos de código que podem se comportar de forma maliciosa antes de serem executados. Ser capaz de aplicar uma análise adicional, inspecionando finamente o comportamento de códigos durante a execução, para detectar comportamento suspeito de aplicações, tais como buffer overflow. Deve possuir técnicas de proteção, que inclui: Análise dinâmica de código - técnica para detectar malware criptografado mais complexo; Algoritmo correspondente padrão - onde os dados de entrada são comparados com um conjunto de sequências conhecidas de código já identificados como um vírus; Emulação - uma técnica para a detecção de vírus polimórficos, ou seja, vírus que se escondem criptografando-se de maneira diferente cada vez que se espalham; Detectar scripts malwares do tipo fileless que possuem seu código obfuscado, inspecionando o código de malwares quando executados diretamente em memória, utilizando os engines de AntiMalware scanning interface (AMSI) ou Early Launch antimalware (ELAM) – EAP Proteção contra malwares que executam payloads que abrem acesso remoto a invasores, ataques conhecidos como shellcode

Serviço Nacional de Aprendizagem Rural

www.senar.org.br

SGAN Quadra 601 Módulo K
Ed. Antônio Ernesto de Salvo
Brasília/DF - CEP 70.830-021
Telefone: (61) 2109-1400

	Proteção contra sequestro de processos do Windows, utilizando a falha do Windows CTF, publicada no CVE-2019-1162. Prevenir tráfego de rede mal-intencionado com inspeção de pacotes de rede Proteção contra-ataques direcionados ao sistema de criptografia do sistema de arquivos (EFS). Bloquear ataques que tentam se passar por processos legítimos do Windows (hollowing); Prevenir a invocação maliciosa de malwares através do Rundll; Detectar e bloquear ameaças que utilizem técnicas de ofuscação e sequestro de DLL Detectar e bloquear técnicas de evasão, incluindo process injection e uso de executáveis legítimos do Windows para rodar scripts e ações maliciosas. Tecnologia de redução de ameaças - detecção de prováveis ameaças por uma variedade de critérios, como extensões duplas (por exemplo. jpg.txt) ou a extensão não coincida com o tipo de arquivo verdadeiro (por exemplo, um arquivo executável ou arquivo .exe com a extensão .txt); Verificação de ameaças web avançadas: bloqueia ameaças verificando o conteúdo em tempo real e remontando com emulação de JavaScript e análise comportamental para identificar e parar o código malicioso de malware avançados;
Funcionalidade de Antivírus e AntiSpyware	Proteção em tempo real contra vírus, trojans, worms, rootkits, botnets, spyware, adwares e outros tipos de códigos maliciosos. Proteção anti-malware deverá ser nativa da solução ou incorporada automaticamente por meio de plug-ins sem a utilização de agentes adicionais, desde que desenvolvidos e distribuídos pelo fabricante. As configurações do anti-spyware deverão ser realizadas através da mesma console do antivírus; Permitir a configuração de ações diferenciadas para programas potencialmente indesejados ou malware, com possibilidade de inclusão de arquivos em listas de exclusão (whitelists) para que não sejam verificados pelo produto; Permitir a varredura das ameaças da maneira manual, agendada e em tempo real na máquina do usuário; Capacidade de detecção e reparo em tempo real de vírus de macro conhecidos e novos através do antivírus; Capacidade de remoção automática total dos danos causados por spyware, adwares e worms, como limpeza do registro e pontos de carregamento, com opção de finalizar o processo e terminar o serviço da ameaça no momento de detecção; A remoção automática dos danos causados deverá ser nativa do próprio antivírus; ou adicionada por plugin, desde que desenvolvido ou distribuído pelo fabricante; Capacidade de bloquear origem de infecção através de compartilhamento de rede com opção de bloqueio da comunicação via rede; Permitir o bloqueio da verificação de vírus em recursos mapeados da rede; Antivírus de Web (verificação de sites e downloads contra vírus); Controle de acesso a sites por categoria; Proteger a navegação na web, mesmo aos usuários fora da rede, para todos os principais navegadores (IE, Firefox, Safari, Opera e Chrome), fornecendo controle da Internet independentemente do browser utilizado, como parte da

Serviço Nacional de Aprendizagem Rural

www.senar.org.br

SGAN Quadra 601 Módulo K
Ed. Antônio Ernesto de Salvo
Brasília/DF - CEP 70.830-021
Telefone: (61) 2109-1400

	solução de proteção a estações de trabalho, incluindo a análise do conteúdo baixado pelo navegador web, de forma independente do navegador usado, ou seja, sem utilizar um plugin, onde não é possível ser ignorada pelos usuários, protegendo os usuários de websites infectados e categorias específicas de websites. O Controle da Web deve controlar o acesso a sites impróprios, com no mínimo 14 categorias de sites inadequados. Deve ainda permitir a criação de lista branca de sites sempre permitidos e lista negra de sites que devem ser bloqueados sempre; Todas as atividades de navegação na Internet bloqueadas deverão ser enviadas para a console de gerenciamento, informando detalhes do evento e a razão para o bloqueio; Capacidade de verificar somente arquivos novos e alterados; Funcionalidades especificas para prevenção contra a ação de ransomwares, tais como a capacidade de impedir a criptografia quando feita por aplicativos desconhecidos ou a capacidade de fazer backup de arquivos antes de serem criptografados para posteriormente permitir sua restauração.
Funcionalidade de detecção Proativa de reconhecimento de novas ameaças e ransomwares	Funcionalidade de detecção de ameaças desconhecidas que estão em memória; Capacidade de detecção, e bloqueio proativo de keyloggers e outros malwares não conhecidos (ataques de dia zero) através da análise de comportamento de processos em memória (heurística); Capacidade de detecção e bloqueio de Trojans e Worms, entre outros malwares, por comportamento dos processos em memória; Capacidade de analisar o comportamento de novos processos ao serem executados, em complemento à varredura agendada. Para estações de trabalho, dispor de capacidade de proteção contra ransomware não baseada exclusivamente na detecção por assinaturas; Para estações de trabalho, dispor de capacidade de remediação da ação de criptografia maliciosa dos ransomwares; Para servidores, dispor de capacidade de prevenção contra a ação de criptografia maliciosa executada por ransomwares, possibilitando ainda o bloqueio dos computadores de onde partirem tal ação.
Funcionalidade de Controle de aplicações e dispositivos	Possuir controle de aplicativos para monitorar e impedir que os usuários executem ou instalem aplicações que podem afetar a produtividade ou o desempenho da rede; Atualiza automaticamente a lista de aplicativos que podem ser controlados, permitindo que aplicativos específicos ou categorias específicas de aplicações possa ser liberada ou bloqueada; Verificar a identidade de um aplicativo de maneira genérica para detectar todas as suas versões. Permitir a solicitação de adição de novas aplicações nas listas de controle de aplicativos através de interface web; Oferecer proteção para chaves de registro e controle de processos; Proibir através de política a inicialização de um processo ou aplicativo baseado em nome e no Hash do arquivo; Detectar aplicativo controlado quando os usuários o acessarem, com as opções de permitir e alertar ou bloquear e alertar; Deve possuir a opção de customizar uma mensagem a ser mostrada ao usuário em caso de bloqueio de execução do aplicativo;

Serviço Nacional de Aprendizagem Rural

www.senar.org.br

SGAN Quadra 601 Módulo K
Ed. Antônio Ernesto de Salvo
Brasília/DF - CEP 70.830-021
Telefone: (61) 2109-1400

	Gerenciar o uso de dispositivos de armazenamento USB (ex: pen-drives e HDs USB). Permitir, através de regras, o bloqueio ou liberação da leitura/escrita/execução do conteúdo desses dispositivos; Controlar o uso de outros dispositivos periféricos, como comunicação infravermelha e modem externo; As funcionalidades do Controle de Aplicações e Dispositivos deverão ser nativas do produto ou incorporadas automaticamente por meio de plug-ins sem utilização de agentes adicionais, desde que desenvolvidos e distribuídos pelo fabricante; Controle de vulnerabilidades do Windows e dos aplicativos instalados; Capacidade de bloquear execução de aplicativo que está em armazenamento externo; A gestão desses dispositivos deverá feita diretamente console de gerenciamento com a possibilidade de definir políticas diferentes por grupos de endpoints; Permitir a autorização de um dispositivo com no mínimo as seguintes opções: Permitir que todos os dispositivos do mesmo modelo; Permitir que um único dispositivo com base em seu número de identificação único; Permitir o acesso total; Permitir acesso somente leitura; Permitir ainda o bloqueio de pontes entre duas redes, por exemplo, um laptop conectado ao mesmo tempo na LAN e se tornar um hotspot Wi-Fi, ou através de um modem.
Funcionalidade de Proteção e Prevenção a Perda de Dados	Possuir proteção a vazamento ou perda de dados sensíveis, considerando o seu conteúdo ou o seu tipo real, além da possibilidade de avaliar a extensão do arquivo e múltiplos destinos como colocado abaixo; Permitir a identificação de informações confidenciais, como números de passaportes ou outras informações pessoais identificáveis e/ou informações confidenciais mesmo que os documentos não tenham sido corretamente classificados, utilizando CCLs (Lista de Controle de Conteúdo); Possibilitar o bloqueio, somente registrar o evento na Console de administração, ou perguntar ao usuário se ele ou ela realmente quer transferir o arquivo identificado como sensível; Deve possuir listas de CCLs pré-configurados com no mínimo as seguintes identificações: Números de cartões de crédito; Números de identificação nacional, como CPF, RG, CNH; Números de contas bancárias; Números de Passaportes; Endereços; Números de telefone; Códigos postais definidas por países como França, Inglaterra, Alemanha, EUA, etc.; Lista de e-mails; Suportar adicionar regras próprias de conteúdo com um assistente fornecido para essa finalidade; Permitir criar regras de prevenção de perda de dados por tipo verdadeiro de arquivo.

Serviço Nacional de Aprendizagem Rural

www.senar.org.br

SGAN Quadra 601 Módulo K
Ed. Antônio Ernesto de Salvo
Brasília/DF - CEP 70.830-021
Telefone: (61) 2109-1400

	Possuir a capacidade de autorizar, bloquear e confirmar a movimentação de dados sensíveis e em todos os casos, gravar a operação realizada com as principais informações da operação; Permitir o controle de dados para no mínimo os seguintes meios: Anexado no cliente de e-mail (ao menos Outlook e Outlook Express); Anexado no navegador (ao menos IE, Firefox e Chrome); Anexado no cliente de mensagens instantâneas (ao menos Skype); Anexado a dispositivos de armazenamento (ao menos USB, CD/DVD).
Características básicas do agente de proteção contra malwares para servidores	A solução deverá ser capaz de proteger servidores contra malwares, arquivos e tráfego de rede malicioso, controle de periféricos, controle de acesso à web, controle de aplicativos em um único agente instalado nos servidores; Deve estar licenciada para pelo menos (01) um servidor para cada localidade/Centro de Excelência. O agente host deve buscar algum sinal de malwares ativos e detectar malwares desconhecidos; O agente deve realizar a atualização várias vezes por dia para manter a detecção atualizada contra as ameaças mais recentes; A solução deve manter conexão direta com banco de dados de ameaças do fabricante para uso da rede de inteligência; Deve realizar a verificação de todos os arquivos acessados em tempo real, mesmo durante o processo de boot; Deve realizar a verificação de todos os arquivos no disco rígido em intervalos programados; Deve realizar a limpeza do sistema automaticamente, removendo itens maliciosos detectados e aplicações potencialmente indesejáveis (PUA); Deve proteger os navegadores Internet Explorer, Firefox, Chrome, Opera e Safari, bloqueando o acesso a sites infectados conhecidos e pela verificação dos dados baixados antes de serem executados; Deve permitir a autorização de detecções maliciosas e excluir da varredura diretórios e arquivos específicos; É requerida a proteção integrada, ou seja, em um único agente, contra ameaças de segurança, incluindo vírus, spyware, trojans, worms, adware e aplicativos potencialmente indesejados (PUAs); O cliente para instalação em estações de trabalho deverá ser compatível com os sistemas operacionais abaixo: Windows Server 2016; Windows Server 2012 R2 (64 bit); Windows Server 2012 (64 bit); Windows Server 2008 R2 (64 bit); Windows Server 2008 (32 or 64 bit); Amazon Linux; CentOS; Novell Open Enterprise Server 2015 SP1; Oracle Linux 6.2/7; Red Hat Enterprise Linux 6/7; SUSE 11/12; Ubuntu Server 14.04/16.04; Deve suportar o uso de servidores usados para atualização em cache para diminuir a largura de banda usada nas atualizações;

Serviço Nacional de Aprendizagem Rural

www.senar.org.br

SGAN Quadra 601 Módulo K
Ed. Antônio Ernesto de Salvo
Brasília/DF - CEP 70.830-021
Telefone: (61) 2109-1400

	Deve possuir integração com as nuvens da Microsoft Azure e Amazon Web Services para identificar as informações dos servidores instanciados nas nuvens; Possuir a funcionalidade de proteção contra a alteração das configurações do agente, impedindo aos usuários, incluindo o administrador local, reconfigurar, desativar ou desinstalar componentes da solução de proteção; Permitir a utilização de senha de proteção para possibilitar a reconfiguração local no cliente ou desinstalação dos componentes de proteção; Deve possuir funcionalidades de monitoração de integridade de arquivos. Deve possuir funcionalidades de whitelistening total do servidor, onde esta funcionalidade atue como um congelamento do servidor, não permitindo que novas aplicações sejam instaladas/executadas sem que seja previamente liberada pela console de gerenciamento da solução; Deve possuir funcionalidades de monitoramento do firewall local do Windows.
Serviço de Instalação	Levantamento de requisitos para a execução; Elaboração de documento contendo as informações sobre o ambiente atual, análise da topologia de rede e apresentação da metodologia de implantação através de projeto de migração; O serviço de implantação deverá ter duração máxima de 15 dias corridos após o início de sua execução; Instalação, configuração e customização da solução. Instalação e configuração do ambiente de gerenciamento; Documentação do ambiente.
Período	O licenciamento e suporte deverão ser no mínimo de 36 (trinta e seis) meses.

LOTE IV – COMPUTADORES	
ITEM 1 – MICROCOMPUTADOR	
QUANTIDADE	**225**
AQUISIÇÃO IMEDIATA: 75 EM TANGARÁ DA SERRA/MT	**75**
Descrição	**PROCESSADOR**: Mínimo 14ª Geração do Processador Intel® Core™ i7 (mínimo de 2,8 GHz, mínimo Turbo Boost 2.0, mínimo 6 Threads 6MB Cache); **MEMÓRIA RAM**: 8 GB de DDR5 a 5600 MHz ou superior; Expansível até 64 GB, (2 slots soDIMM) com suporte a Dual Channel; **ARMAZENAMENTO**: Mínimo SSD M.2 NVMe PCIe 256 GB unidade de estado sólido integrado (não serão aceitos adaptadores, conectores, interfaces, encaixes, acopladores, ou plugues para realizar adequações ou quaisquer ajustes); **TELA MONITOR**: LED Tipo LCD retro iluminado LED/WLED; Widescreen 16:9; Tamanho 21.5"; Ajustes de Altura, rotação, giratório e inclinação; Relação de contraste mínimo 1000:1; com mínimo 02 (duas) entradas de sinal de imagem: (DisplayPort + HDMI ou DisplayPort + DisplayPort ou DVi + DisplayPort) e mínimo 04 portas USB Type A 3.2; (com os cabos de conexão equivalentes e totalmente compatíveis ao modelo de placa de vídeo oferecida no microcomputador ofertado);

Serviço Nacional de Aprendizagem Rural

www.senar.org.br

SGAN Quadra 601 Módulo K
Ed. Antônio Ernesto de Salvo
Brasília/DF - CEP 70.830-021
Telefone: (61) 2109-1400

	TECLADO: padrão ABNT2 português conexão USB com fio; Cor Preta; **MOUSE**: óptico; USB com fio; Cor Preta; **PLACA DE VÍDEO**: Integrada Intel® HD (DisplayPort + HDMI ou DisplayPort + DisplayPort ou DVi + DisplayPort); **PLACA CONTROLADORA DE ÁUDIO:** Porta combinada no painel frontal de entrada/saída interface de áudio para headset universal de 3,5 mm (P2); **MODELO DE GABINETE**: Formato (MFF -Mini Form Factor), Cor Preta; sensor de intrusão integrado, slot de segurança Kensington e projeto Tool-Less; Dispositivos originais do fabricante, não sendo aceitas quaisquer adaptações no gabinete; Podendo ser utilizado nas posições horizontal, vertical e afixado ao monitor com através do suporte específico; **SUPORTE:** Deve permitir a fixação do gabinete na parte traseira ou na base do monitor ofertado, sem interferir nos ajustes de altura, inclinação ou rotação do monitor. O suporte deve ser da mesma marca do fabricante do monitor, possuir furação VESA compatível para fixação do gabinete e incluir todos os acessórios e parafusos necessários para sua instalação e utilização; **CONECTIVIDADE**: Gigabit (RJ-45) com padrão Ethernet 10/100/1000 Mbps; Placa Wi-Fi padrão (802.11ax) interface interna M2 e Bluetooth versão 5.1 integrados, ou superior; **PORTAS INTEGRADAS**: Painel frontal 2 portas USB sendo: 01 Type A 3.2 e 01 USB Type-C 3.2 (10Gbit/s), não sendo permitida a utilização de adaptadores. Painel traseiro mínimo de 04 portas USB (02 portas USB 3.2 de 1ª geração e 02 USB 2.0), 01 porta DisplayPort 1.4a, 01 RJ45 Ethernet, 01 HDMI e 01 porta de alimentação; **MODELO DE GABINETE**: Desktop – (MFF - Micro Form Factor) Cor Preta; **FONTE DE ALIMENTAÇÃO**: CA bivolt automático - mínimo 65W; **SISTEMA OPERACIONAL**: Windows 11 Professional, em português Brasil 64bits com o licenciamento perpétuo; **SOFTWARE DE RECUPERAÇÃO DO EQUIPAMENTO DO PRÓPRIO FABRICANTE**: Permitir retornar o equipamento à sua configuração de software Sistema operacional original de fábrica, caso ocorra falha que exija reinstalação sem a necessidade de intervenção para configuração de drivers, dispositivos e programas instalados; **CERTIFICAÇÃO 1**: O fabricante dos equipamentos deverá estar relacionado no web site da EICC, http://www.eiccoalition.org/about/members ou apresentar o **Certificado da OHSAS 18001** válido; **CERTIFICAÇÃO 2:** A (s) empresa (s) primeira colocada do(s) lote(s) referido(s) acima deverão apresentar a certificação do fabricante com o modelo do equipamento ofertado registrado no EPEAT (*Electronic Product Environmental Assessment Tool*) da Agência de Proteção Ambiental (EPA), nas categorias Bronze, Silver ou Gold, e estar listada e cadastrada no site: http://www.epeat.net, comprovando que o equipamento atinge as exigências para controle do impacto ambiental em seu processo de fabricação ou certificação emitida pelo INMETRO ou entidade credenciada por este Instituto, em conformidade com a Portaria n.º 170, de 10 de abril de 2012. **CERTIFICAÇÃO 3:** Possuir a certificação ISO 14001 e 9001 do fabricante;

Serviço Nacional de Aprendizagem Rural

www.senar.org.br

SGAN Quadra 601 Módulo K
Ed. Antônio Ernesto de Salvo
Brasília/DF - CEP 70.830-021
Telefone: (61) 2109-1400

	CERTIFICAÇÃO 4: O licitante deverá comprovar que o fabricante dos equipamentos possui cadastro na organização de padrões DMTF em Member List na categoria "Board" e estar relacionado no web site https://www.dmtf.org/about/list; **CERTIFICAÇÃO 5**: Apresentar certificação ENERGY STAR do equipamento ofertado. Este certificado deverá ser comprovado através do web site http://www.energystar.gov. Sendo necessário identificar a marca e o modelo ou família do equipamento; O fabricante deve ser registrado na "Membership List" do Unified Extensible Firmware Interface Fórum, acessível pela web site http://www.uefi.org/members, estando na categoria "PROMOTERS", de forma a atestar que os seus equipamentos estão em conformidade com a especificação UEFI 2.x ou superior. Deverá ser apresentada comprovação em que o fabricante do equipamento é membro do consorcio DMTF (desktop management task force). O fabricante deverá ser membro na categoria "BOARD". Esta exigência deverá ser conferida através do web site http://www.dmtf.org/about/list / onde o fabricante deverá pertencer a categoria solicitada; O fabricante do equipamento deverá ser membro da EICC ou possuir Certificação válida OHSAS 18001, para garantia de conformidade com as questões ambientais, qualidade e segurança do bem-estar de seus funcionários e investimentos ambientais. O fabricante deverá estar relacionado na web site da EICC, http://www.eiccoalition.org/about/members ou apresentar o Certificado da OHSAS 18001 válido. **Obs.:** • Será exigida a comprovação de autorização para comercializar os equipamentos ofertados, podendo ser através de declaração do fabricante ou do distribuidor autorizado do fabricante; Relação de assistência técnica nacional do fabricante. • O gabinete, mouse, teclado, monitor (tela) deverão ser na cor PRETA e da mesma; marca do fabricante do equipamento; • A Placa mãe deverá ser do mesmo fabricante do equipamento; • Possuir integrado e dedicado à placa principal SafeID inclui módulo TPM – Trusted Platform Module 2.0; • Modelos normativos de referência: Para MICROCOMPUTADOR: Modelo normativo: D15U, Tipo normativo: D15U005, Dell OptiPlex 7020 MFF (Formato micro), TELA MONITOR: Dell P2222H; • A licitante vencedora deverá fornecer o equipamento completo de amostra para homologação e validação da equipe técnica em até 5 dias corridos após a solicitação e antes da assinatura do contrato. Obs.: O kit mouse, teclado e monitor (tela) deverão ser na cor PRETA e da mesma marca do fabricante do computador.
Garantia e Níveis de Serviço (SLA)	
Período	A garantia do equipamento deverá ser on-site e de mínimo de 36 (trinta e seis) meses.

Serviço Nacional de Aprendizagem Rural

www.senar.org.br

SGAN Quadra 601 Módulo K
Ed. Antônio Ernesto de Salvo
Brasília/DF - CEP 70.830-021
Telefone: (61) 2109-1400

Atendimento	Suporte técnico dedicado e especializado, in loco, para reparos deverá ser no regime de 7x24 e ser realizado diretamente por um técnico especializado pelo fabricante do equipamento ou pela contratada, caso o fabricante a tenha certificado para tal.
Cobertura	A garantia e suporte deverá cobrir todos os itens que compõem o equipamento (hardware e software).
Chamado	A abertura de chamados deverá correr através de chamada telefônica para o número fixo, regime 7x24. Opcionalmente os chamados poderão ser abertos on-site.

LOTE IV – NOTEBOOK	
ITEM 2 -NOTEBOOK	
QUANTIDADE	**48**
AQUISIÇÃO IMEDIATA: 16 EM TANGARÁ DA SERRA/MT	**16**
Descrição	**PROCESSADOR**: Mínimo 14ª Geração do Processador Intel® Core™ i7 (mínimo de 3,0 GHz, mínimo Turbo Boost 2.0, mínimo 4 Threads 4MB Cache); **MEMÓRIA RAM**: Mínimo de 32 GB DDR5 a 5600 MHz; **ARMAZENAMENTO**: Mínimo SSD M.2 NVMe PCIe 512 GB unidade de estado sólido; **TELA MONITOR:** LED de 14" 16:9, Full HD Touch (1920 x 1080), antibrilho, câmera integrada de alta definição 1080p e microfone integrado; **TECLADO:** Padrão ABNT2 português (Brasil); iluminado, Touchpad incorporado; **MOUSE:** Mouse sem fio com sensor led óptico, dois botões (direito e esquerdo), Scroll de rolagem mecânica, alimentação 01 pilha AA, com interface de conexão 2.4 GHz receptor USB e Bluetooth 5.0 ou superior, botão liga/desliga e de alternância, resolução de movimento mínimo 1600 ppp; Cor: Preta; Do mesmo fabricante do notebook; **PLACA DE VÍDEO**: integrada Intel® HD; **WEBCAM**: integrada de 1080p; **CONECTIVIDADE**: Gigabit (RJ-45) com padrão Ethernet 10/100/1000 Mbps; Placa Wi-Fi padrão (802.11ax) interface interna e Bluetooth versão 5.1 integrados, ou superior; **PORTAS INTEGRADAS:** Mínimo 02 Portas USB 3.2 de 1ª geração (01 com PowerShare), 01 HDMI 2.0, 01 RJ45 e 02 USB 3.2 Type-C de 1ª geração; **ÁUDIO:** Alto-falantes integrados estéreo duplo mínimo de 2 W; Entrada e Saída de Áudio para Fone e microfone Plug P2 Integrado; **OUTROS**: Mochila (bag) para transporte com compatibilidade para notebooks entre 15 e 16 polegadas, Dimensões aproximadas: Altura: 40-45 cm, Largura: 30-35 cm, Profundidade: 15-20 cm, Peso: Aproximadamente 600g a 1kg, Resistente a água, Ergonomia: Alças ajustáveis e acolchoadas para maior conforto, Puxadores e alças superiores reforçadas, Compartimentos organizados para itens pessoais e acessórios eletrônicos, Forro interno acolchoado para proteção contra impactos, Cor: Preta, da mesma marca do fabricante do equipamento; **BATERIA:** Recarregável com no mínimo 3 células, lithium-ion, 41 Whr; **FONTE DE ALIMENTAÇÃO:** Mínimo de 60 W AC adapter, USB-C, bivolt – automático da mesma marca do fabricante;

Serviço Nacional de Aprendizagem Rural

www.senar.org.br

SGAN Quadra 601 Módulo K
Ed. Antônio Ernesto de Salvo
Brasília/DF - CEP 70.830-021
Telefone: (61) 2109-1400

	SISTEMA OPERACIONAL: Windows 11 Professional, em português Brasil 64bits com o licenciamento perpétuo; **SOFTWARE DE RECUPERAÇÃO DO EQUIPAMENTO DO PRÓPRIO FABRICANTE**: Permitir retornar o equipamento à sua configuração de software Sistema operacional original de fábrica, caso ocorra falha que exija reinstalação sem a necessidade de intervenção para configuração de drivers, dispositivos e programas instalados. **CERTIFICAÇÃO 1**: O fabricante dos equipamentos deverá estar relacionado na web site da EICC, http://www.eiccoalition.org/about/members ou apresentar o **Certificado da OHSAS 18001** válido; **CERTIFICAÇÃO 2:** A (s) empresa (s) primeira colocada do(s) lote(s) referido(s) acima deverão apresentar a certificação do fabricante com o modelo do equipamento ofertado registradono EPEAT (*Electronic Product Environmental Assessment Tool*) da Agência de Proteção Ambiental (EPA), nas categorias Bronze, Silver ou Gold, e estar listada e cadastrada no site: http://www.epeat.net, comprovando que o equipamento atinge as exigências para controle do impacto ambiental em seu processo de fabricação ou certificação emitida pelo INMETRO ou entidade credenciada por este Instituto, em conformidade com a Portaria n.º 170, de 10 de abril de 2012. **CERTIFICAÇÃO 3:** Possuir a certificação ISO 14001 e 9001 do fabricante; **CERTIFICAÇÃO 4:** O licitante deverá comprovar que o fabricante dos equipamentos possui cadastro na organização de padrões DMTF em Member List na categoria "Board" e estar relacionado no web site https://www.dmtf.org/about/list; **CERTIFICAÇÃO 5**: Apresentar certificação ENERGY STAR do equipamento ofertado. Este certificado deverá ser comprovado através do web site http://www.energystar.gov. Sendo necessário identificar a marca e o modelo ou família do equipamento; O fabricante deve ser registrado na "Membership List" do Unified Extensible Firmware Interface Fórum, acessível pela web site http://www.uefi.org/members, estando na categoria "PROMOTERS", de forma a atestar que os seus equipamentos estão em conformidade com a especificação UEFI 2.x ou superior. Deverá ser apresentada comprovação em que o fabricante do equipamento é membro do consorcio DMTF (desktop management task force). O fabricante deverá ser membro na categoria "BOARD". Esta exigência deverá ser conferida através do web site http://www.dmtf.org/about/list / onde o fabricante deverá pertencer a categoria solicitada; O fabricante do equipamento deverá ser membro da EICC ou possuir Certificação válida OHSAS 18001, para garantia de conformidade com as questões ambientais, qualidade e segurança do bem-estar de seus funcionários e investimentos ambientais. O fabricante deverá estar relacionado na web site da EICC, http://www.eiccoalition.org/about/members ou apresentar o Certificado da OHSAS 18001 válido. **Obs.:** • Será exigida a comprovação de autorização para comercializar os equipamentos ofertados, podendo ser através de declaração do fabricante ou do distribuidor autorizado do fabricante; Relação de assistência técnica nacional do fabricante.

Serviço Nacional de Aprendizagem Rural

www.senar.org.br

SGAN Quadra 601 Módulo K
Ed. Antônio Ernesto de Salvo
Brasília/DF - CEP 70.830-021
Telefone: (61) 2109-1400

	• O gabinete do notebook deverá ser na cor PRETA, GRAFITE ou CINZA. Modelo normativo de referência: P165G - DELL LATITUDE 5440 ou superior.
Garantia e Níveis de Serviço (SLA)	
Período	A garantia do equipamento deverá ser on-site e de mínimo de 36 (trinta e seis) meses.
Atendimento	Suporte técnico dedicado e especializado, in loco, para reparos deverá ser no regime de 7x24 e ser realizado diretamente por um técnico especializado pelo fabricante do equipamento ou pela contratada, caso o fabricante a tenha certificado para tal.
Cobertura	A garantia e suporte deverá cobrir todos os itens que compõem o equipamento (hardware e software).
Chamado	A abertura de chamados deverá correr através de chamada telefônica para o número fixo, regime 7x24. Opcionalmente os chamados poderão ser abertos on-site.

LOTE V – TV DE LED 65 POLEGADAS	
TV LED FULL HD	
QUANTIDADE	**48**
AQUISIÇÃO IMEDIATA: 16 EM TANGARÁ DA SERRA/MT	**16**
Descrição	**TAMANHO**: 65"; **TIPO:** Smart 4K QNED; **Frequência Nativa:** 60Hz nativo; **Saída de Áudio:** Sim **CONEXÕES:** Mínima de 2 HDMI, 2 USB, 1 Ethernet (Lan); **Wi-Fi:** Sim; **COMPATÍVEL COM APPLE AIRPLAY2**: Sim; **RESOLUÇÃO (Mínima):** Full HD 1.920 X 1.080 linhas (2.073.600 pixels); **SISTEMA DE TV:** ISDB-TB, PAL-N, PAL-M, NTSC; **CABO DE ALIMENTAÇÃO**: Sim; **ALIMENTAÇÃO**: Fonte de alimentação bivolt automático 100 - 240 V AC;
Geral	Modelo normativo de referência: Smart TV LG QNED AI 4K - QNED85 65" 2024.
Garantia e Níveis de Serviço (SLA)	
Período	A garantia do equipamento deverá ser on-site e de mínimo de 12 (doze) meses.
Atendimento	O atendimento deverá ser no regime de 7x24 a ser realizado diretamente pelo fabricante do equipamento ou pela contratada, caso o fabricante a tenha certificado para tal.
Cobertura	A garantia deverá cobrir todos os itens que compõem o equipamento.
Chamado	A abertura de chamados deverá correr através de chamada telefônica para o número fixo, regime 7x24. Opcionalmente os chamados poderão ser abertos através do site na Internet.

Serviço Nacional de Aprendizagem Rural

www.senar.org.br

SGAN Quadra 601 Módulo K
Ed. Antônio Ernesto de Salvo
Brasília/DF - CEP 70.830-021
Telefone: (61) 2109-1400

LOTE VI – PROJETOR LASER	
PROJETOR LASER 4.600 LÚMENS EM CORES E 4.600 LÚMENS EM BRANCO	
QUANTIDADE	**03**
AQUISIÇÃO IMEDIATA: 01 EM TANGARÁ DA SERRA/MT	**01**
Especificação	**SISTEMA DE PROJEÇÃO TECNOLOGIA:** 3LCD de 3 chips; **MODO DE PROJEÇÃO:** Frontal/traseiro/instalado no teto; **VISOR:** LCD 0,62-polegadas (C2fine); **MÉTODO DE PROJEÇÃO:** Matriz ativa TFT de polissilício; **NÚMERO DE PIXELS:** 2.073.600 pixels (1920 x 1080) x 3; **RESOLUÇÃO NATIVA:** Full HD 1080p; **RELAÇÃO DE ASPECTO:** 16:9, 16:10, 21:9; **BRILHO EM CORES:** 4.600 lúmens; **BRILHO EM BRANCO:** 4.600 lúmens; **RELAÇÃO DE CONTRASTE:** Até 2.500.000:1; **REPRODUÇÃO DE CORES:** Até 1 bilhão de cores; **ALTO-FALANTE MONAURAL:** 16W x 1; **RUÍDO DO VENTILADOR:** 27 dB / 37 dB; **CERTIFICAÇÕES E NORMAS:** Estar de acordo e serem fornecidos conforme norma NBR 14136:2002, lei nº 11.337 de 26 de julho de 2006 e resolução CONMETRO nº 02, de 06 de setembro de 2007 publicado no D.O.U 14.09.2009; O equipamento deve atender à diretiva RoHS (Restriction of Hazardous Substances), em conformidade com a IN01 de 19/01/2010 da SLTI/MP (TI Verde), quanto a não utilização de substâncias nocivas ao Meio Ambiente ou deve ser apresentada comprovação técnica demonstrando que o equipamento não é fabricado utilizando substâncias nocivas ao Meio Ambiente como cádmio (Cd), mercúrio (Hg), cromo hexavalente (Cr(VI)), bifenilos polibromados (PBBs), éteres difenil-polibromados (PBDEs) e chumbo (Pb);
Lente de projeção	**TIPO:** Zoom não óptico(manual)/Foco (manual); **DISTÂNCIA FOCAL:** 18,2 mm - 29,1 mm; **RELAÇÃO DE ZOOM:** 1 - 1,62; **RELAÇÃO DE TIRO:** 1,32 - 2,12; **TAMANHO DA IMAGEM:** 31" a 310" (88 cm a 906 cm); **DISTÂNCIA DE PROJEÇÃO PARA IMAGEM PADRÃO:** 62" 1,80 m; **CORREÇÃO DE KEYSTONE:** +/-30 graus a +/-30 graus; **QUICK CORNER:** Sim;
Conectividade	D-sub 15 pinos VGA - Entrada: 2; RCA Composto Vídeo In: 1; HDMI: 2; D-sub 15 pinos VGA - Saída: 1; Entrada de Áudio RCA (Vermelho/Branco): 1; Entradas de Áudio (Stereo mini de 3,5 mm): 2; Saída de Áudio (Stereo mini de 3,5mm): 1; RS-232C: 1; USB Tipo A (para módulo sem fio): 1; USB Tipo B: 1; RJ45: 1; Módulo sem fio: Integrado; Wi-Fi Certified™ Miracast®: Sim;
Energia	**TENSÃO DE FONTE DE ALIMENTAÇÃO:** 100 V AC-240 V AC +/- 10%, 50/60 Hz; **TIPO DE FONTE DE ILUMINAÇÃO:** Diodo Laser; **VIDA ÚTIL DA FONTE DE ILUMINAÇÃO NORMAL**: 20.000 horas/ **ESTENDIDO:** 30.000 horas; **CONSUMO DE ENERGIA:** 272 W (normal) – 208 W (Silencioso);
Geral	**TEMPERATURA DE OPERAÇÃO:** 0 °C a 40 °C; **DIMENSÕES (L X A X P):** 325 mm x 105 mm x 299 mm;

Serviço Nacional de Aprendizagem Rural

www.senar.org.br

SGAN Quadra 601 Módulo K
Ed. Antônio Ernesto de Salvo
Brasília/DF - CEP 70.830-021
Telefone: (61) 2109-1400

	PESO: 4,2 kg; **SEGURANÇA:** Trava Kensington barra de segurança e Criptografia de Segurança de Nível Empresarial; **ACIONAMENTO BOTOEIRA:** Três posições Sobe/Para/Desce, cabeada, integrada; **CONTROLE REMOTO:** Sim; **PILHAS DO CONTROLE REMOTO:** Incluso; **CABO DE ALIMENTAÇÃO:** 1 unidade; **CABO HDMI:** 1 unidade; **MODELO NORMATIVO DE REFERÊNCIA**: EPSON PowerLite L260F ou superior;
Garantia e Níveis de Serviço (SLA)	
Período	A garantia deverá ser de mínimo de 36 (trinta e seis) meses ou 20.000 horas.
Atendimento	O atendimento deverá ser no regime de 7x24 a ser realizado diretamente pelo fabricante do equipamento ou pela contratada, caso o fabricante a tenha certificado para tal.
Cobertura	A garantia deverá cobrir todos os itens que compõem o equipamento.

LOTE VII – TELA DE PROJEÇÃO	
TELA DE PROJEÇÃO ELÉTRICA TENSIONADA 120 POLEGADAS	
QUANTIDADE	**03**
AQUISIÇÃO IMEDIATA: 01 EM TANGARÁ DA SERRA/MT	**01**
Descrição	**TELA:** Elétrica tensionada (120" HDTV 16x9); **TECIDO:** Matte White Flex – Ganho de 1.1 (Branca com verso Preto); **DIMENSÕES (Área de Projeção):** Largura 261 cm x Altura 150,5 cm x Diagonal 301 cm x Polegadas 120"; **ESTOJO:** Em alumínio; **PINTURA:** Eletrostática na cor branca **BORDAS:** Pretas **MOTOR:** Tubular interno, silencioso com Velocidade de 34RPM e Torque de 10Nm - Voltagem 220v **ACIONAMENTO:** Controle remoto sem fio; **TENSIONAMENTO:** Ajustável; **CONTROLE REMOTO:** Sim - Com sistema de Rádio Frequência **SUPORTE:** Trilho corrediço em toda extensão do Estojo da tela; **MODELO NORMATIVO DE REFERÊNCIA: TELA** de Projeção Elétrica – Tensionada;
Garantia e Níveis de Serviço (SLA)	
Período	A garantia do equipamento deverá ser on-site e de mínimo de 12 (doze) meses.
Cobertura	A garantia deverá cobrir todos os itens que compõem o equipamento.

6. PRAZO DE ENTREGA

Os equipamentos deverão ser entregues no prazo máximo de **30 (trinta) dias,** a contar do recebimento da Autorização de Compra ou Autorização de Fornecimento, devendo a (s) entrega (s) ser (em) agendada (s)

Serviço Nacional de Aprendizagem Rural

www.senar.org.br

SGAN Quadra 601 Módulo K
Ed. Antônio Ernesto de Salvo
Brasília/DF - CEP 70.830-021
Telefone: (61) 2109-1400

previamente, com antecedência de pelo menos 72 (setenta e duas) horas, pelo telefone **(61) 2109-1499** e pelo e-mail **senar.informatica@senar.org.br**.

7. ASPECTOS GERAIS

7.1. Todos os equipamentos e seus componentes/periféricos entregues à CONTRATANTE devem ser originais de fábrica e novos (sem uso, reforma ou recondicionamento) em regime normal de produção, sendo produto novo e comercializado normalmente através dos canais de revenda do fabricante;

7.2. Os equipamentos deverão ser entregues com todos os itens acessórios de hardware e software necessários à sua perfeita ativação e funcionamento, incluindo cabos, adaptadores e conectores, interfaces, suportes, drivers de controle, programa de configuração entre outros, necessários ao perfeito funcionamento dos mesmos;

7.3. Na eventualidade de um dos itens do objeto não estar mais disponível no mercado, a CONTRATADA deverá substituir por um com a mesma qualidade e especificação técnica do produto fora de linha ou superior;

7.4. A CONTRATADA deverá entregar os equipamentos, para homologação pela área técnica da CONTRATANTE nos locais definidos nas Autorizações de Compra. Deve acompanhar prospecto (documentação técnica) com as características técnicas detalhadas dos equipamentos, especificando Marca, Modelo, Código do produto e outros elementos que de forma inequívoca identifiquem e constatem as configurações cotadas, possíveis expansões e “upgrades”, comprovando-os através de “folders” e demais literaturas técnicas editadas pelos fabricantes. Serão aceitas cópias das especificações obtidas no sitio na Internet do fabricante juntamente com o endereço do sitio.

8. DA GARANTIA

8.1. Os equipamentos deverão possuir garantia do fabricante, definidos em cada Lote/Item deste TR, contados a partir do recebimento definitivo do objeto, sem prejuízo de qualquer política de garantia adicional oferecido pelo fabricante. A LICITANTE deverá descrever em sua proposta, o termo de garantia adicional oferecido pelo fabricante e o processo de atendimento;

8.2. A garantia deverá ser prestada, sem qualquer ônus adicional ao Senar, diretamente pelo fabricante ou por sua rede de assistência técnica autorizada;

8.3. Eventuais custos de transporte, estadia, remessa de peças necessárias à manutenção corretiva dos equipamentos serão custeados pelo fornecedor, durante todo o período de garantia do equipamento, caso estas não sejam cobertas ou pelo fabricante ou por sua rede de assistência técnica autorizada;

8.4. Entende-se por manutenção corretiva aquela decorrente de defeitos de fabricação ou por defeito identificado durante ou após a instalação.

9. DO SERVIÇO DE ATENDIMENTO E DE SUPORTE TÉCNICO

9.1. A LICITANTE VENCEDORA deverá entregar (com fornecimento de todo o material necessário) nos endereços descritos no item 11. DOS LOCAIS DE FORNECIMENTO E INSTALAÇÃO os equipamentos e programas solicitados e Declaração da CONTRATADA, apresentando a (s) empresa (s) responsável (is) pela Assistência Técnica autorizada na cidade de entrega, contendo os seguintes dados:

Serviço Nacional de Aprendizagem Rural

www.senar.org.br

SGAN Quadra 601 Módulo K
Ed. Antônio Ernesto de Salvo
Brasília/DF - CEP 70.830-021
Telefone: (61) 2109-1400

- Razão social, C.N.P.J., endereço, CEP, telefone e e-mail;
- Nome do responsável técnico e do representante legal;

9.2. A abertura e o gerenciamento de chamados e suporte técnico serão realizados diretamente pelo fabricante ou Assistência Técnica Autorizada dos equipamentos por meio de número telefônico fornecido pela CONTRATADA;

9.3. O fabricante e a CONTRATADA devem garantir a existência de peças para reposição, bem como, a expansão ou atualização dos equipamentos, por um período não inferior ao de garantia;

9.4. O SLA de atendimento será de 8x5x24, ou seja, o atendimento será no horário comercial das 9h às 18h, nos dias úteis, com prazo de solução de 48 (quarenta e oito) horas a partir da abertura do chamado;

9.5. O término do reparo do equipamento não poderá ultrapassar o prazo previsto de SLA, caso contrário deverá ser providenciado, pela CONTRATADA, a substituição do equipamento por um equivalente ou de superior configuração como backup, até que seja sanado o defeito do equipamento.

10. DA VIGÊNCIA DO REGISTRO DE PREÇOS

Este Registro de Preços terá vigência de 12 (doze) meses, podendo ser prorrogado até o limite de 36 (trinta e seis) meses, desde que, o resultado da pesquisa de mercado demonstre que o custo-benefício se mantém vantajoso.

11. DOS LOCAIS DE FORNECIMENTO E INSTALAÇÃO

a) Centro de Excelência em Grãos, Fibras e Oleaginosas: Anel Viário André Antônio Maggi, n° 2930-W. Bairro: Parque da Serra – Tangará da Serra/MT – CEP: 78.305-500.

b) Centro de Excelência em Zootecnia: Parque de Exposições João Martins da Silva, BR 324 - KM 521, Subaé - Feira de Santana/BA - CEP: 44.079-002.

c) Centro de Excelência em Cana de Açucar: Avenida Brasil, 2000 localizada no bairro Vila Elisa, na cidade de Ribeirão Preto/SP - CEP: 14.075-030.

d) SENAR/Administração Central: SGAN Quadra 601, Módulo K - Edifício Antônio Ernesto de Salvo, Brasília - DF - CEP: 70.830-021.

12. DAS AUTORIZAÇÕES DE COMPRA

As Aquisições, objeto deste Termo de Referência, serão executadas a partir da emissão de Autorizações de Compras pelo CONTRATANTE, especificadas em cada Lote e Item, de acordo com a necessidade do Senar, sendo que as quantidades estimadas para entrega imediata nos locais previamente definidos neste Termo de Referência poderão ser alteradas pela CONTRATANTE.

13. DA EMISSÃO DA NOTA FISCAL

13.1. As Notas Fiscais deverão ser emitidas em favor do Senar/Administração Central, com sede em Brasília/DF, e as entregas deverão ser realizadas nos locais definidos no item 11 deste Termo de Referência, devidamente detalhados nas Autorizações de Compras.

Serviço Nacional de Aprendizagem Rural

www.senar.org.br

SGAN Quadra 601 Módulo K
Ed. Antônio Ernesto de Salvo
Brasília/DF - CEP 70.830-021
Telefone: (61) 2109-1400

13.2. Todas as despesas inerentes à entrega nos estados, tais como Frete, Instalação e Impostos, dentre outras, deverão estar contempladas na Proposta de Preços apresentada pela LICITANTE.

Serviço Nacional de Aprendizagem Rural

www.senar.org.br

SGAN Quadra 601 Módulo K
Ed. Antônio Ernesto de Salvo
Brasília/DF - CEP 70.830-021
Telefone: (61) 2109-1400