TERMO DE REFERÊNCIA (BASEADO NO DECRETO n. 15477/2020 E SEUS ANEXOS)

1. DECLARAÇÃO DO OBJETO

1.1 Contratação de empresa especializada para fornecimento de solução envolvendo hardware, software, assinaturas de atualização, instalação, treinamento, customização e suporte em proteção e otimização de tráfego em redes WAN e proteção multicamadas contra ameaças avançadas em mensagens, conforme especificações técnicas, incluindo os appliances necessários e suficientes para a prestação desses serviços, para atender às demandas e necessidades da SEFAZ-MS pelo período de 12 (doze) meses.

1.2 Planilha de itens da contratação:

Item	Especificação	Unid.	Qtd.	Vl. Unit.	Vl. Total.
001	Contratação de empresa especializada em serviço de tecnologia da informação	Mês	12		

1.3 A contratação será via Licitação na modalidade Pregão Eletrônico, conforme a Lei Federal nº 8.6668/93, Lei Federal nº 10.520/2002 e Decreto Estadual 15.327/2019;

2. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

2.1 O presente termo de referência visa descrever a necessidade da SGI/SEFAZ/MS em contratar uma solução de TIC que forneça para as redes WAN da Secretaria de Estado de Fazenda, os seguintes recursos finalísticos:

2.1.1 Aceleração e otimização de tráfego de dados em redes WAN, através de análise de conteúdo de aplicações;

2.1.2 Proteção de rede multicamadas para ameaças avançadas em tráfego de mensagens eletrônicas para redes WAN;

2.1.3 Alta disponibilidade de rede, em modo Ativo/Standby;

2.1.4 Recurso de VPN entre dispositivos de mesmo fabricante e de outros fabricantes, usando padrão IPSEC;

2.1.5 Proteção do ambiente para ataques internos e externos, através de funcionalidades de Firewall e de IPS integrado;

2.1.6 Reconhecimento, gerenciamento e bloqueio de aplicações, com independência de porta e protocolo.

2.1.7 Filtragem de URL para gerenciamento e controle de acessos.

2.1.8 Proteção antivírus e anti-bot;

2.1.9 Inspeção de tráfego de entrada e saída de malwares não conhecidos ou do tipo APT;

2.1.10 Gerenciamento de toda a infraestrutura fornecida, através de software acessível através de plataforma única de administração de todos os produtos instalados.

2.2 A solução deverá ser fornecida com os serviços necessários à sua sustentação, sendo estes:

2.2.1 Serviço de garantia de hardware para toda a infraestrutura fornecida;

2.2.2 Suporte técnico do fabricante, necessário para manutenção da garantia dos equipamentos e softwares;

2.2.3 Atualização de novas versões de software, durante o período de vigência do contrato;

2.2.4 Acesso a base de conhecimento ou semelhante, para orientação e transferência de conhecimento da solução pela equipe técnica da SGI/SEFAZ;

2.2.5 Treinamento para instalação, configuração e operação (administração) da solução;

2.2.6 A Contratada deverá fornecer qualquer licenciamento necessário para prover todos os recursos descritos neste documento.

3. JUSTIFICATIVA DO OBJETO

3.1 O Governo do Estado de Mato Grosso do Sul, através da Superintendência de Gestão da Informação – SGI/SEFAZ/MS está em constante processo de atualização tecnológica de seus sistemas de informação, programas e softwares legados, que gradativamente estão sendo substituídos por soluções computacionais em plataforma Web e *Mobile*, proporcionando assim maior escalabilidade e portabilidade aos serviços públicos digitais, através de acesso por diversas plataformas e dispositivos conectados através de Intranet e/ou Internet, objetivando assim o melhor atendimento às necessidades dos usuários internos e o aumento da capilaridade dos serviços públicos disponíveis à sociedade.

3.2 Considerando a abrangência das ações do Secretaria de Estado de Fazenda em toda a extensão territorial do Estado, as soluções de TIC desenvolvidas pela SGI/SEFAZ são utilizadas diuturnamente em todos os municípios, principalmente nas Agências

Fazendárias, Postos de Atendimento SEFAZ, Unidades de Fiscalização e Controle e Postos Fiscais.

3.3 Como em todo sistema de informação, os dados produzidos e manipulados são armazenados e processados em bancos de dados gerenciais, que no âmbito do Governo Estadual são armazenados de forma centralizada em seu Datacenter, nas dependências da Superintendência de Gestão da Informação em Campo Grande/MS.

3.4 Neste cenário, para prover o acesso a estes sistemas, bem como a outros softwares armazenados no Datacenter, incluindo correio eletrônico, Intranet e demais ferramentas de software, a SEFAZ/MS mantém contrato com operadoras de telecomunicação (Telecom), para dispor de circuitos de comunicação de dados que integram o núcleo da rede de computadores (Datacenter) a cada uma das localidades atendidas pelo órgão.

3.5 O fato é que a infraestrutura fornecida por estas operadoras carece de recursos computacionais robustos, necessários para o tráfego intenso e crítico de dados produzido nas rotinas de trabalho diário. Por questões de limitação de tecnologia e extensão geográfica do País, as Telecom fornecem recursos insuficientes de largura de banda, transporte seguro de dados e latência dos circuitos, e a custos elevados, principalmente quando se trata de localidades alheias aos grandes centros no Sul e Sudeste brasileiros.

3.6 Ainda neste contexto, há muitos problemas de atendimento por parte das operadoras devido ao limite da capacidade da rede de telecomunicações instalada nas cidades do interior do Estado, o que prejudica enormemente o tempo de resposta de acesso aos sistemas, programas e softwares desenvolvidos e disponibilizados em rede WAN.

3.7 Diante desse desafio, é necessário a contratação de soluções tecnológicas e serviços para auxiliar na transposição das barreiras de acesso às soluções de TIC, que suportam a execução dos procedimentos administrativos internos da Secretaria e do atendimento ao contribuinte.

3.8 O objetivo esperado com esta contratação é obter solução que maximize a produtividade dos colaboradores e proporcionar uma melhor experiência de trabalho com acessos aos sistemas, programas e softwares de forma mais ágil, reduzindo a latência de rede e melhorando o tempo de resposta das aplicações desenvolvidas, bem como fornecer uma camada de proteção destes circuitos, dos dados e das mensagens eletrônicas trafegadas na rede WAN, garantindo melhor segurança e desempenho.

3.9 O dimensionamento da solução pretendida foi realizado com base no cenário levando em consideração as necessidades atuais da infraestrutura e com provisionamento para futuras ampliações no ambiente da SEFAZ/MS.

3.10 É importante salientar que, por se tratar de um serviço agregador, de modernização do ambiente atual e da infraestrutura tecnológica do Governo do Estado de Mato Grosso do Sul, todo o investimento outrora realizado em outras iniciativas será integralmente aproveitado, não havendo danos causados pela contratação destes serviços à infraestrutura existente. Muito pelo contrário, a proposta visa a integração nativa aos sistemas em uso, sem a necessidade de se alterar linhas de código ou configurações do ambiente existente.

3.11 Todo o serviço se adaptará aos usuários de modo geral de forma a garantir proteção e desempenho no acesso às informações. Desta forma, teremos uma visão unificada do comportamento do serviço de aceleração e otimização que fará parte do pacote proposto. Além disto, a arquitetura permitirá a integração com outros sistemas de monitoração e virtualização de ambiente, devido à flexibilidade na customização dos cenários.

4. ESPECIFICAÇÃO DO OBJETO

4.1 REQUISITOS LEGAIS:

4.1.1 Lei n. 9.472, de 16 de julho de 1997.

4.1.2 Resolução n. 715, de 23 de outubro de 2019, da Agência Nacional de Telecomunicações.

4.1.3 Todos os produtos de hardware componentes da solução deverão ser homologados e certificados pela ANATEL, conforme preceitua o art. 19, incisos XIII e XIV, e art. 156 da Lei n. 9.472, de 16 de julho de 1997 e ainda pelos art. 55, art. 64, inciso II e art. 67, parágrafo 2° da Resolução ANATEL n. 715, de 23 de outubro de 2019.

4.2 REQUISITOS DE ARQUITETURA TECNOLÓGICA:

4.2.1 Requisitos Específicos para o Appliance do SITE CENTRAL (SGI):

4.2.1.1 Requisitos de Capacidade e de Interfaces:

4.2.1.1.1 Os requisitos mínimos exigidos neste subitem são justificados pela necessidade de garantir que a solução ofertada possua: a) capacidade de operação redundante (energia e refrigeração) provendo resiliência e tolerância à falhas; b) processamento, largura de banda e taxa de transferência suficiente para suportar o alto volume de dados trafegados na rede da SEFAZ/MS pelos diversos sistemas e softwares utilizados; e c) a quantidade de interfaces de rede necessárias para suportar toda a arquitetura do ambiente funcional da rede no núcleo da SGI, permitindo o devido gerenciamento, monitoramento e operação da solução sem necessidade de adaptações ou equipamentos sobressalentes;

4.2.1.1.2 A solução ofertada deverá ser fornecida com configuração de hardware para cluster em redundância/alta disponibilidade com, no mínimo, 02 (dois) equipamentos;

4.2.1.1.3 Performance de Firewall Stateful Packet Inspection igual ou superior a 15 Gbps;

4.2.1.1.4 Performance de IPS de 5 Gbps ou superior;

4.2.1.1.5 Suporte a, no mínimo, 5.000.000 (cinco milhões) de conexões do tipo SPI simultâneas;

4.2.1.1.6 Suporte a, no mínimo, 1.500.000 (um milhão e quinhentos mil) conexões do tipo DPI simultâneas;

4.2.1.1.7 Suporte a, no mínimo, 100.000 (cem mil) novas conexões por segundo;

4.2.1.1.8 Fonte de alimentação redundante, com chaveamento automático de 100-240 e hot-swappable;

4.2.1.1.9 Possuir redundância do sistema de refrigeração do produto (Fan) redundante com, no mínimo, dois ventiladores;

4.2.1.1.10 Deverá possuir pelo menos quatro interfaces de 10 GbE SFP+;

4.2.1.1.11 Deverá possuir pelo menos oito interfaces de 1 GbE SFP;

4.2.1.1.12 Suportar, no mínimo, 8 interfaces 10/100/1000 Gbe. Todas as interfaces devem possuir mecanismo de autosense e seleção de modo half/full duplex. A seleção da velocidade e duplex deve ser realizada

obrigatoriamente através da interface gráfica de gerenciamento. As interfaces devem suportar as seguintes atribuições:

4.2.1.1.12.1 Segmento WAN, ou externo;

4.2.1.1.12.2 Segmento WAN, secundário com possibilidade de ativação de recurso para redundância de WAN com balanceamento de carga e WAN Failover por aplicação. O equipamento deverá suportar no mínimo balanceamento de 4 links utilizando diferentes métricas pré-definidas pelo sistema e configuráveis pelo administrador;

4.2.1.1.12.3 Segmento LAN ou rede interna;

4.2.1.1.12.4 Segmento LAN ou rede interna podendo ser configurado como DMZ (Zona desmilitarizada);

4.2.1.1.12.5 Segmento LAN ou rede interna ou Porta de sincronismo para funcionamento em alta disponibilidade;

4.2.1.1.12.6 Segmento ou Zona exclusiva para controle de dispositivos Wireless dedicado, com controle e configuração destes dispositivos.

4.2.1.1.13 01 (uma) interface de rede dedicada para gerenciamento;

4.2.1.1.14 01 (uma) interface do tipo console ou similar;

4.2.1.1.15 A VPN SSL deve ser licenciada para, no mínimo, 2 (dois) usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para, no mínimo, 3.000 (três mil) usuários simultâneos, com aquisição de licença futura;

4.2.1.1.16 Suportar 10.000 (dez mil) túneis de VPN IPSEC simultâneos;

4.2.1.1.17 Suportar, no mínimo, 5 Gbps de throughput de VPN IPSEC;

4.2.1.1.18 Performance para inspeção de Anti-Malware integrado no mesmo appliance de 3.5 Gbps ou superior.

4.2.1.2 Requisitos Gerais:

4.2.1.2.1 Os requisitos mínimos exigidos neste subitem são justificados pelas necessidades de: a) contratar uma solução específica de mercado, com tecnologia construída para os fins a que se destinam, através de um processo de engenharia de qualidade, e não um produto adaptado em cima de um hardware ou software genérico, sem garantia de

desempenho ou da qualidade de seus componentes; e b) garantir que o produto ofertado tenha as funcionalidades mínimas necessárias para qualquer hardware desta finalidade e que possam ser configurados de acordo com a especificidade da rede de dados WAN da SEFAZ/MS, independentemente de mudanças futuras na topologia da rede;

4.2.1.2.2 Todas as funcionalidades descritas devem funcionar no mesmo appliance sem a necessidade de composição de um ou mais produtos;

4.2.1.2.3 A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7 (modelo OSI);

4.2.1.2.4 O hardware e software que executem as funcionalidades de proteção de rede devem ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;

4.2.1.2.5 O equipamento deverá ser baseado em hardware desenvolvido com está finalidade, ou seja, não sendo aceita soluções baseadas em plataforma PC ou equivalente;

4.2.1.2.6 Não serão permitidas soluções baseadas em sistemas operacionais abertos (OpenSource) como Free BSD, Debian ou mesmo Linux;

4.2.1.2.7 Todo o ambiente deverá ser gerenciado através de uma única interface sem a necessidade de produtos de terceiros para compor a solução;

4.2.1.2.8 Deve ser possível suportar arquitetura de armazenamento de logs redundante, permitindo a configuração de equipamentos distintos;

4.2.1.2.9 A solução deverá suportar monitoramento através de SNMP v2 e v3;

4.2.1.2.10 Deve oferecer as funcionalidades de backup/restore tanto da configuração quanto do firmware/sistema operacional através da interface gráfica, assim como permitir ao administrador agendar procedimentos de backups da configuração em determinado dia e hora;

4.2.1.2.11 O appliance deve armazenar, no mínimo, 02 (duas) versões distintas do sistema operacional, sendo possível escolher qual versão será inicializada; de backups da configuração em determinado dia e hora;

4.2.1.2.12 Suporte à definição de VLAN no firewall, conforme padrão IEEE 802.1q e ser possível criar sub-interfaces lógicas associadas a VLANs e estabelecer regras de filtragem (Stateful Firewall) entre elas;

4.2.1.2.13 A solução deve suportar configuração de link-aggregation de interfaces suportando o protocolo 802.3ad para aumento de throughput;

4.2.1.2.14 A solução deve suportar configuração de port-redundacy de interfaces para a alta disponibilidade de interfaces;

4.2.1.2.15 Os dispositivos de proteção devem ter a capacidade de operar de forma simultânea mediante o uso de suas interfaces físicas nos seguintes modos:

4.2.1.2.15.1 Modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3);

4.2.1.2.15.2 Modo sniffer, para inspeção via porta espelhada do tráfego de dados da rede;

4.2.1.2.15.3 Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;

4.2.1.2.15.4 Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas;

4.2.1.2.15.5 Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas.

4.2.1.2.16 Possuir DHCP Server interno;

4.2.1.2.17 Suporte a encaminhamento de pacotes UDPs multicast/broadcast entre diferentes interfaces e zonas de segurança como como DHCP Relay, suportando os protocolos e portas: Time service—UDP porta 37, DNS—UDP porta 53, DHCP—UDP portas 67 e 68, Net-Bios DNS—UDP porta 137, Net-Bios Datagram—UDP porta 138, Wake On LAN—UDP porta 7 e 9, mDNS—UDP porta 5353;

4.2.1.2.18 Suporte a Jumbo Frames;

4.2.1.2.19 Implementar sub-interfaces ethernet lógicas;

4.2.1.2.20 Deve suportar os seguintes tipos de NAT: Nat dinâmico (Many-to-1); Nat dinâmico (Many-to-Many); Nat estático (1-to-1); NAT estático (Many-to-Many); Nat estático bidirecional 1-to-1; Tradução de porta (PAT); NAT de origem; NAT de destino;

4.2.1.2.21 Suportar NAT de origem e NAT de destino simultaneamente;

4.2.1.2.22 Prover mecanismo contra-ataques de falsificação de endereços (IP Spoofing);

4.2.1.2.23 Implementar mecanismo de sincronismo de horário através do protocolo NTP. Para tanto o appliance deve realizar a pesquisa em pelo menos 03 servidores NTP distintos, com a configuração do tempo do intervalo de pesquisa;

4.2.1.2.24 Possuir gerenciamento de tráfego de entrada ou saída, por serviços, endereços IP e regra de firewall, permitindo definir banda mínima garantida e máxima permitida em porcentagem (%) para cada regra definida;

4.2.1.2.25 Implementar 802.1p e classe de serviços CoS (Class of Service) de DSCP (Differentiated Services Code Points);

4.2.1.2.26 Permitir remarcação de pacotes utilizando TOS e/ou DSCP;

4.2.1.2.27 Suporte a policy based routing (PBR), com a capacidade de roteamento por endereço de origem, endereço de destino, serviço, interface ou todas as opções simultâneas;

4.2.1.2.28 Suporte ao protocolo de roteamento multicast (PIM-SM);

4.2.1.2.29 Suportar protocolos de roteamento RIP, RIPng, OSPF, OSPFv3 e BGP;

4.2.1.2.30 Suportar Equal Cost Multi-Path (ECMP);

4.2.1.2.31 Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);

4.2.1.2.32 Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3, RIPng);

4.2.1.2.33 A solução deve suportar integralmente o padrão IPv6, assim como criação de regras com objetos que utilizem endereços IPv4 e IPv6;

4.2.1.2.34 Deve suportar no mínimo as seguintes funcionalidades ou protocolos para o padrão de endereçamento IPv6: Tunel 6 to 4, regras de acesso, objetos de endereço, limitador de conexões IPv6, monitor de conexões, DHCP, gerenciamento HTTPS via IPv6, NAT IPv6, proteção contra ataques do tipo IP Spoofing para IPv6, captura de pacotes IPv6, interface VLAN com endereço IPv6, VPN SSL com o uso do IPv6, controle de URL, Anti-Malware e anti-virus, controle de aplicação, IPS, IKEv2, ICMP6, SNMP, alta disponibilidade, RFC 1981 Path MTU Discovery for IPv6, RFC 2460 IPv6 specification, RFC 2464 Transmission of IPv6 Packets over Ethernet Networks;

4.2.1.2.35 Possui suporte a log via syslog;

4.2.1.2.36 Possuir mecanismo para possibilitar a aplicação de correções e atualizações para o firewall remotamente através da interface gráfica;

4.2.1.2.37 Permitir a visualização em tempo real de todas as conexões TCP e sessões UDP que se encontrem ativas através do firewall;

4.2.1.2.38 A tecnologia deve possuir, pelo menos, uma certificação da ICSA Labs, ICSA Firewall ou Antivirus;

4.2.1.2.39 O fabricante da solução deverá ser avaliado pela NSS Labs (Network Security Services) no desempenho do Next Generation Firewall Comparative Analysis mais recente, estando no “Security Value Map” acima de 90% (noventa por cento) da avaliação de segurança efetiva.

4.2.1.2.40 Permitir a geração de gráficos em tempo real, representando os serviços mais utilizados e as máquinas mais acessadas em um dado momento;

4.2.1.2.41 Permitir a visualização de estatísticas do uso de CPU do appliance o através da interface gráfica remota em tempo real.

4.2.1.3 Requisitos de Alta Disponibilidade:

4.2.1.3.1 Os requisitos mínimos exigidos neste subitem são justificados pela necessidade de garantia da disponibilidade da solução em caso de queda de um dos equipamentos instalados no Site Central (SGI), ou seja, a solução deve automaticamente se manter operacional na ocorrência de qualquer evento que ocasione a parada de um dos itens da solução;

4.2.1.3.2 A solução deve possuir mecanismo de Alta Disponibilidade operando em modo Ativo/Standby, com as implementações de Fail Over;

4.2.1.3.3 Não serão permitidas soluções de cluster (HA) que façam com que o equipamento reinicie após qualquer modificação de parâmetro/configuração realizada pelo administrador;

4.2.1.3.4 O recurso de Alta Disponibilidade deverá ser suportado em modo Bridge.

4.2.1.4 Requisitos de VPN (Virtual Private Network):

4.2.1.4.1 Os requisitos mínimos exigidos neste subitem são justificados pela necessidade que a solução proporcione recursos de VPN, para interconexão das diversas localidades atendidas de maneira segura, provendo criptografia e sigilosidade no tráfego de dados entre o Site Central e os demais sites da rede WAN da SEFAZ/MS, através de tecnologia usual de mercado e não proprietária;

4.2.1.4.2 Criptografia 3DES, AES 128 e AES 256;

4.2.1.4.3 Autenticação com MD5, SHA-1, SHA-256 e SHA-384;

4.2.1.4.4 Diffie-Hellman: Grupo 2 (1024 bits), Grupo 5 (1536 bits) e Grupo 14 (2048 bits;

4.2.1.4.5 Algoritmo Internet Key Exchange (IKE);

4.2.1.4.6 Autenticação via certificado IKE PKI;

4.2.1.4.7 Deve possuir interoperabilidade com outros fabricantes de acordo com o padrão IPSEC através de RFC`s;

4.2.1.4.8 A solução deve suportar VPNs L2TP, incluindo suporte para iPhone, Windows phone, Android com suporte a cliente L2TP;

4.2.1.4.9 Solução deve suportar VPNs baseadas em políticas e VPNs baseadas em roteamento estático e dinâmico;

4.2.1.4.10 Suportar políticas de roteamento sobre conexões VPN IPSEC do tipo site-to-site com diferentes métricas e serviços. A rota poderá prover aos usuários diferentes caminhos redundantes sobre todas as conexões VPN IPSEC;

4.2.1.4.11 Solução deve incluir a capacidade de estabelecer VPNs com outros firewalls que utilizam IP públicos dinâmicos;

4.2.1.4.12 Permitir a definição de um gateway redundante para terminação de VPN no caso de queda do circuito primário;

4.2.1.4.13 Permitir que seja criado políticas de roteamentos estáticos utilizando IPs de origem, destino, serviços e a própria VPN como parte encaminhadora deste tráfego sendo este visto pela regra de roteamento, como uma interface simples de rede para encaminhamento do tráfego;

4.2.1.4.14 Suportar a criação de túneis IP sobre IP (IPSEC Tunnel), de modo a possibilitar que duas redes com endereço inválido possam se comunicar através da Internet.

4.2.1.5 Requisitos de Autenticação:

4.2.1.5.1 Os requisitos mínimos exigidos neste subitem são necessários para garantir autenticidade (controle de acesso), através da autenticação dos usuários da rede, evitando acesso indevido de usuários ou de equipamentos não autorizados às informações trafegadas entre as localidades da rede WAN da SEFAZ/MS e o Site Central, e especificam tecnologias padrão de mercado e utilizadas no âmbito do parque computacional do Estado;

4.2.1.5.2 Permitir a utilização de LDAP, AD e RADIUS;

4.2.1.5.3 Permitir o cadastro manual dos usuários e grupos diretamente na interface de gerencia remota do Firewall, caso onde se dispensa um autenticador remoto para o mesmo;

4.2.1.5.4 Suporte a uma rede com múltiplos domínios, possibilitando a integração em um ambiente onde existas domínios diferentes e totalmente segregados.

4.2.1.5.5 Permitir a integração com qualquer autoridade certificadora emissora de certificados X509 que seguir o padrão de PKI descrito na RFC 2459, inclusive verificando as CRLs emitidas periodicamente pelas autoridades, que devem ser obtidas automaticamente pelo firewall via protocolos HTTP e LDAP;

4.2.1.5.6 Permitir o controle de acesso por usuário, para plataformas Windows Me, NT, 2000, XP, Windows 7, Windows 8 e Windows 10 de forma transparente, para todos os serviços suportados, de forma que ao efetuar o logon na rede, um determinado usuário tenha seu perfil de acesso automaticamente configurado;

4.2.1.5.7 Permitir a restrição de atribuição de perfil de acesso a usuário ou grupo independente ao endereço IP da máquina que o usuário esteja utilizando.

4.2.1.5.8 Suportar recurso de autenticação única para todo o ambiente de rede, ou seja, utilizando a plataforma de autenticação atual que pode ser de LDAP ou AD; o perfil de cada usuário deverá ser obtido automaticamente através de regras no Firewall DPI (Deep Packet Inspection) sem a necessidade de uma nova autenticação como por exemplo, para os serviços de navegação a Internet atuando assim de forma toda transparente ao usuário. Serviços como HTTP, HTTPS devem apenas consultar uma base de dados de usuários e grupos de servidores 2008/2012 com AD.

4.2.1.6 Requisitos de IPS (Intrusion Prevention System):

4.2.1.6.1 Os requisitos mínimos exigidos neste subitem são necessários para garantir proteção à rede, contra os ataques do tipo intrusão, inspecionando todos os pacotes trafegados para agir preventiva e pró-ativamente nas ocorrências de tentativa de invasão à rede WAN, e são as especificações mínimas para produtos desta natureza;

4.2.1.6.2 Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS integrados no próprio appliance de firewall, onde sua console de gerência deverá residir na mesma console centralizada dos appliances de segurança, com suporte a pelo menos 3.000 assinaturas;

4.2.1.6.3 A solução de IPS deverá possuir os seguintes mecanismos de detecção: assinaturas e trabalhar em conjunto com o controle de aplicações;

4.2.1.6.4 A solução de IPS deve fazer a inspeção de todo o pacote, independentemente do tamanho;

4.2.1.6.5 A solução de IPS deve fazer a inspeção de todo o trafego de forma bidirecional, analisando qualquer tamanho de pacote sem degradar a performance do equipamento;

4.2.1.6.6 Possuir capacidade de remontagem de pacotes para identificação de ataques;

4.2.1.6.7 O mecanismo de inspeção deve receber e implementar em tempo real atualizações para os ataques emergentes sem a necessidade de reiniciar o appliance;

4.2.1.6.8 Para cada proteção de segurança, deve ser possível consultar informações no site do fabricante;

4.2.1.6.9 A ferramenta de log deve possuir a capacidade de criar uma regra de exceção a partir do log visualizado na gerência centralizada;

4.2.1.6.10 As regras de exceção devem possuir: origem, destino e serviço;

4.2.1.6.11 A solução deve ser capaz de inspecionar tráfego HTTPS;

4.2.1.6.12 Deverá possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep;

4.2.1.6.13 Deverá possuir capacidade de detecção de anomalias;

4.2.1.6.14 A solução de IPS deve possuir política capaz de definir o modo de operação (bloqueio ou detecção);

4.2.1.6.15 O módulo de IPS deve possuir assinaturas voltadas para ambientes de servidores de SMTP, Web e DNS;

4.2.1.6.16 O mecanismo de inspeção deve receber e implementar em tempo real atualizações de novas assinaturas sem a necessidade de reiniciar o appliance;

4.2.1.6.17 Para cada proteção, ou para todas as proteções suportadas, deve incluir a opção de adicionar exceções baseado na origem e destino;

4.2.1.6.18 A solução deve ser capaz de detectar e bloquear ataques nas camadas de rede e aplicação, protegendo pelo menos os seguintes serviços:

Aplicações web, serviços de e-mail, DNS, FTP, SQL Injection, ataques a sistemas operacionais e VOIP;

4.2.1.6.19 Deve incluir proteção contra worms;

4.2.1.6.20 Deve incluir uma tela de visualização situacional a fim de monitorar graficamente a quantidade de alertas de diferentes severidades e a evolução ao longo do tempo dispondo o sumario quantitativo das ameaças analisadas;

4.2.1.6.21 A solução deve possuir esquema de atualização de assinaturas através de um click;

4.2.1.6.22 Atualização de modo offline, onde poderá ser baixado na base do fabricante e posteriormente fazer o upload do arquivo na solução;

4.2.1.6.23 A solução deve suportar importar certificados de servidor para inspeções de tráfego seguro HTTP (HTTPS) de entrada. Depois de importar esses certificados, a solução deve permitir o IPS para Inspeção segura HTTP (HTTPS);

4.2.1.6.24 A solução deverá ser capaz de inspecionar e proteger apenas hosts internos;

4.2.1.6.25 A solução deverá possuir proteções para sistemas SCADA;

4.2.1.6.26 Solução deverá permitir que o administrador bloqueie facilmente o tráfego de entrada e/ou saída com base em países, sem a necessidade de gerir manualmente os ranges de endereços IP dos países que deseja bloquear;

4.2.1.6.27 Possibilitar operação em modo de detecção baseado em base de assinaturas SNORT.

4.2.1.7 Requisitos de Controle de Aplicação:

4.2.1.7.1 Os requisitos mínimos exigidos neste subitem são necessários para prover recursos de gerenciamento das aplicações (sistemas, softwares, etc.) que trafegam pelos circuitos gerenciados, possibilitando à equipe técnica da SGI a liberação de aplicações confiáveis e o bloqueio daquelas alheias à atividade laboral ou que gerem ameaças de segurança ao Site

Central, independentemente desta utilizar porta ou protocolo de rede de outra aplicação liberada (análise dos pacotes de dados);

4.2.1.7.2 Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;

4.2.1.7.3 Deve ser possível a liberação e bloqueio de aplicações sem a necessidade de liberação de portas e protocolos;

4.2.1.7.4 Capacidade para realizar filtragens/inspeções dentro de portas TCP conhecidas por exemplo porta 80 http, buscando por aplicações que potencialmente expõe o ambiente como: P2P, Kazaa, Morpheus, BitTorrent ou messengers;

4.2.1.7.5 Controlar o uso dos serviços de Instant Messengers como MSN, YAHOO, Google Talk, ICQ, de acordo com o perfil de cada usuário ou grupo de usuários, de modo a definir, para cada perfil, se ele pode ou não realizar download e/ou upload de arquivos, limitar as extensões dos arquivos que podem ser enviados/recebidos e permissões e bloqueio de sua utilização baseados em horários pré-determinados pelo administrador será obrigatório para este item;

4.2.1.7.6 Deverá controlar software FreeProxy tais como ToR, Ultrasurf, Freegate, etc;

4.2.1.7.7 Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;

4.2.1.7.8 Deverá permitir a criação de regras para acesso/bloqueio por subrede de origem e destino;

4.2.1.7.9 Atualizar a base de assinaturas de aplicações automaticamente;

4.2.1.7.10 Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos do LDAP/AD;

4.2.1.7.11 A solução de controle de aplicação WEB deve criar regras granulares possibilitando adicionar tipos de aplicação WEB e categorias por regra, sendo assim criando controle granular de qualquer tipo de acesso não permitido pela empresa;

4.2.1.7.12 Deve implementar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e protocolos;

4.2.1.7.13 Caso a solução não tenha assinaturas pré-definida na solução a mesma deverá possibilitar a criação ou importação de assinaturas personalizadas para os seguintes tipos ou protocolos: HTTP, FTP, E-mail e extensão de arquivos;

4.2.1.7.14 O administrador deve ser capaz de configurar quais comandos FTP são aceitos e quais são bloqueados a partir de comandos FTP pré-definidos;

4.2.1.7.15 Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;

4.2.1.7.16 Deverá possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, uTorrent, etc.) possuindo granularidade de controle/políticas para os mesmos;

4.2.1.7.17 Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Facebook e bloquear chat;

4.2.1.7.18 Deverá possibilitar a diferenciação de aplicações Proxies possuindo granularidade de controle/políticas para os mesmos;

4.2.1.7.19 Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como:

4.2.1.7.19.1 Nível de risco da aplicação.

4.2.1.7.19.2 Categoria de aplicações.

4.2.1.8 Requisitos de Filtragem de URL (Uniform Resource Locator):

4.2.1.8.1 Os requisitos mínimos exigidos neste subitem são necessários para prover recurso de controle e gerenciamento de sites Web visitados pelos usuários, proporcionando a criação de políticas de filtragem de conteúdo ilegal, imoral, indevido ou alheio a execução das atividades laborais, garantindo assim conformidade às políticas e normas de segurança e evitando desvios de conduta;

4.2.1.8.2 Para prover maior visibilidade e controle dos acessos dos usuários do ambiente, deve ser incluído um módulo de filtro de URL integrado no firewall;

4.2.1.8.3 Possuir base contendo no mínimo 20 milhões de sites internet web já registrados e classificados com atualização automática;

4.2.1.8.4 Implementar filtro de conteúdo transparente para o protocolo HTTP, de forma a dispensar a configuração dos browsers das máquinas clientes;

4.2.1.8.5 Permitir a criação de listas personalizadas de URLs permitidas e bloqueadas (lista branca e lista negra) ;

4.2.1.8.6 Permitir especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora).

4.2.1.8.7 Deve ser possível à criação de políticas por usuários, grupos de usuários, IPs, redes e grupos de redes;

4.2.1.8.8 O mecanismo de Controle de aplicação Web/URL deve apresentar contagem de utilização de regra de acordo com a utilização (hit count);

4.2.1.8.9 Deverá permitir criar política de confirmação de acesso;

4.2.1.8.10 Deve possibilitar a inspeção de tráfego HTTPS (Inbound/Outbound), sendo que para a opção de Outbound não será necessário efetuar o "man-inthe- middle", ou seja, a solução deverá prover mecanismo que irá analisar a conexão HTTPS para verificar se a URL solicitada está na lista de permissões de acesso, de acordo com a política configurada;

4.2.1.8.11 O administrador poderá adicionar filtros por palavra-chave de modo específico;

4.2.1.8.12 Deverá permitir o bloqueio Web através de senha pré configurada pelo administrador;

4.2.1.8.13 Deverá permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que, antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);

4.2.1.8.14 A solução deve fornecer um mecanismo para solicitação de categorização de URL caso esta não esteja categorizada ou categorizada incorretamente;

4.2.1.8.15 Suportar recurso de autenticação única para todo o ambiente de rede, ou seja, utilizando a plataforma de autenticação atual que pode ser de LDAP ou AD; o perfil de cada usuário deverá ser obtido automaticamente para o controle das políticas de Filtro de Conteúdo sem a necessidade de uma nova autenticação;

4.2.1.8.16 Suportar a criação de políticas baseadas no controle por URL e categoria de URL;

4.2.1.8.17 Suportar base ou cache de URLs local no appliance ou possibilitar a replicação da base de conhecimento de URLs do fabricante via instalação de máquina virtual, a infraestrutura da máquina virtual (VM) para uso desse recurso será fornecida pelo Contratante, evitando delay de comunicação/validação das URLs;

4.2.1.8.18 Possuir pelo menos 50 categorias de URLs;

4.2.1.8.19 Suporta a criação de categorias de URLs customizadas;

4.2.1.8.20 Suporta a exclusão de URLs do bloqueio, por categoria;

4.2.1.8.21 Deverá possibilitar a categorização ou recategorização de URL caso não esteja categorizada ou categorizada incorretamente;

4.2.1.8.22 A solução deverá permitir um mecanismo que permita sobrescrever as categorias de URL;

4.2.1.8.23 Permitir a customização de página de bloqueio.

4.2.1.9 Requisitos de Proteção Contra Vírus e Botnets:

4.2.1.9.1 Os requisitos mínimos exigidos neste subitem são justificados pela necessidade de proteger o ambiente de rede WAN de ataques dos tipos “vírus” e “botnets”, que podem acarretar na perda de informação crítica, roubo de dados sigilosos, degradação de serviços ou interrupção de funcionamento de sistemas de informações e equipamentos essenciais para continuidade dos serviços públicos prestados, e

constituem especificações usuais e padrão de mercado para tecnologias com esta finalidade;

4.2.1.9.2 Deve possuir módulo de antivírus e anti-bot integrado no próprio appliance de segurança;

4.2.1.9.3 A solução deve possuir nuvem de inteligência proprietária do fabricante onde seja responsável em atualizar toda a base de segurança dos appliances através de assinaturas;

4.2.1.9.4 Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e qualquer outro mecanismo de redirecionamento de tráfego;

4.2.1.9.5 Implementar funcionalidade de detecção e bloqueio de callbacks;

4.2.1.9.6 A solução deverá ser capaz de detectar e bloquear comportamento suspeito ou anormal da rede;

4.2.1.9.7 A solução anti-bot deve possuir mecanismo de detecção que inclui, reputação de endereço IP;

4.2.1.9.8 Implementar interface gráfica WEB segura, utilizando o protocolo HTTPS;

4.2.1.9.9 Implementar interface CLI segura através do protocolo SSH;

4.2.1.9.10 Possuir antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, IMAP, POP3, FTP, CIFS e TCP Stream;

4.2.1.9.11 A solução deve permitir criar regras de exceção de acordo com a proteção;

4.2.1.9.12 Deve possuir visualização na própria interface de gerenciamento referente aos top incidentes através de hosts ou incidentes referentes a incidentes de vírus e Bots;

4.2.1.9.13 Permitir o bloqueio de malwares (vírus, worms, spyware e etc) ;

4.2.1.9.14 A solução deve ser capaz de proteger contra ataques para DNS;

4.2.1.9.15 A solução deverá ser gerenciada a partir de uma console centralizada com políticas granulares;

4.2.1.9.16 A solução deve ser capaz de prevenir acesso a websites maliciosos;

4.2.1.9.17 A solução deve ser capaz de realizar inspeção de tráfego SSL e SSH;

4.2.1.9.18 A solução deverá receber atualizações de um serviço baseado em cloud;

4.2.1.9.19 A solução deverá ser capaz de bloquear a entrada de arquivos maliciosos;

4.2.1.9.20 A solução Antivírus deverá suportar análise de arquivos que trafegam dentro do protocolo CIFS;

4.2.1.9.21 A solução deve suportar funcionalidade de GeoIP, ou seja, a capacidade de identificar, isolar e controlar tráfego baseado na localização (origem e/ou destino), incluindo a capacidade de configuração de listas customizadas para esta mesma finalidade.

4.2.1.10 Requisitos de Proteção para Ataques Avançados:

4.2.1.10.1 Os requisitos mínimos exigidos neste subitem são justificados pela necessidade de proteger o ambiente de rede WAN de ataques dos tipos “APT Malware”, “ameaças de dia zero” e “ameaças não conhecidas”, através da inspeção avançada de tráfego, inclusive criptografado, detectando anomalias e comportamentos suspeitos de aplicações, e que também podem acarretar na perda de informação crítica, roubo de dados sigilosos, degradação de serviços ou interrupção de funcionamento de sistemas de informações e equipamentos essenciais para continuidade dos serviços públicos prestados, e constituem especificações usuais e padrão de mercado para tecnologias com esta finalidade;

4.2.1.10.2 A solução deverá prover as funcionalidades de inspeção de tráfego de entrada e saída de malwares não conhecidos ou do tipo APT com filtro de ameaças avançadas e análise de execução em tempo real, e inspeção de tráfego de saída de callbacks;

4.2.1.10.3 Suportar os protocolos HTTP assim como inspeção de tráfego criptografado através de HTTPS e TLS;

4.2.1.10.4 A solução deve ser capaz de inspecionar o tráfego criptografado SSL e SSH;

4.2.1.10.5 Identificar e bloquear a existência de malware em comunicações de entrada e saída, incluindo destinos de servidores do tipo Comando e Controle;

4.2.1.10.6 Implementar mecanismo de bloqueio de vazamento não intencional de dados oriundos de máquinas existentes no ambiente LAN em tempo real;

4.2.1.10.7 Implementar detecção e bloqueio imediato de malwares que utilizem mecanismo de exploração em arquivos no formato PDF, sendo que a solução deve inspecionar arquivo PDF com até 10Mb;

4.2.1.10.8 Implementar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows XP, Windows 7, Windows 10, MacOS, Android, Linux;

4.2.1.10.9 Conter ameaças de dia zero permitindo ao usuário final o recebimento dos arquivos livres de malware;

4.2.1.10.10 A tecnologia de máquina virtual deverá suportar diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso sem utilização de assinaturas;

4.2.1.10.11 A solução deve possuir nuvem de inteligência proprietária do fabricante onde seja responsável em atualizar toda a base de segurança dos appliance através de assinaturas.

4.2.1.10.12 Implementar a visualização dos resultados das análises de malwares de dia zero nos diferentes sistemas operacionais dos ambientes controlados (sandbox) suportados;

4.2.1.10.13 Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e qualquer outro mecanismo de redirecionamento de tráfego;

4.2.1.10.14 Conter ameaças avançadas de dia zero;

4.2.1.10.15 Toda análise deverá ser realizada de forma automatizada sem a necessidade de criação de regras específicas e/ou interação de um operador;

4.2.1.10.16 Implementar mecanismo do tipo múltiplas fases para verificação de malware e/ou códigos maliciosos;

4.2.1.10.17 Toda a análise e bloqueio de malwares e/ou códigos maliciosos deve ocorrer em tempo real. Não serão aceitas soluções que apenas detectam o malware e/ou códigos maliciosos;

4.2.1.10.18 Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx) e Android APKs no ambiente controlado;

4.2.1.10.19 Implementar a análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL no ambiente controlado;

4.2.1.10.20 Possuir antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, POP3, FTP, IMAP e CIFS;

4.2.1.10.21 Conter ameaças de dia zero de forma transparente para o usuário final;

4.2.1.10.22 Conter ameaças de dia zero através de tecnologias em nível de emulação e código de registro;

4.2.1.10.23 Implementar mecanismo de pesquisa por diferentes intervalos de tempo;

4.2.1.10.24 Conter ameaças de dia zero via tráfego de internet;

4.2.1.10.25 Permitir a contenção de ameaças de dia zero sem a alteração da infraestrutura de segurança;

4.2.1.10.26 Conter ameaças de dia zero que possam burlar o sistema operacional emulado;

4.2.1.10.27 A solução deve permitir a criação de whitelist baseado no MD5 do arquivo;

4.2.1.10.28 Conter ameaças de dia zero antes da execução e evasão de qualquer código malicioso;

4.2.1.10.29 Conter exploits avançados;

4.2.1.10.30 A análise “In Cloud” ou local deve prover informações sobre as ações do Malware na máquina infectada, informações sobre quais aplicações são utilizadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo Malware, gerar assinaturas de Antivírus e

Antispyware automaticamente, definir URLs não confiáveis utilizadas pelo novo Malware e prover Informações sobre o usuário infectado (seu endereço IP e seu login de rede);

4.2.1.10.31 Suporte a submissão manual de arquivos para análise através do serviço de Sandbox.

4.2.1.11 Requisitos de Administração:

4.2.1.11.1 Os requisitos mínimos exigidos neste subitem são justificados pela necessidade da equipe técnica da SGI em administrar a solução instalada no Site Central, através de uma interface integrada e com todos os recursos e funcionalidades fornecidos pela solução, com disponibilidade de acesso local e/ou remoto e capacidade de gerenciar a todos os usuários (colaboradores diretos e terceirizados) que utilizam a rede de dados da SEFAZ/MS;

4.2.1.11.2 Suportar no mínimo 80.000 usuários autenticados com serviços ativos e identificados;

4.2.1.11.3 Políticas baseadas por grupos de usuários deverão ser suportadas;

4.2.1.11.4 Permitir a criação de perfis de administração distintos, de forma a possibilitar a definição de diversos administradores para o firewall, cada um responsável por determinadas tarefas da administração;

4.2.1.11.5 Fornecer gerência remota, com interface gráfica nativa;

4.2.1.11.6 A interface gráfica deverá possuir assistentes para facilitar a configuração inicial e a realização das tarefas mais comuns na administração do firewall, incluindo a configuração de VPN IPSECs, NAT, perfis de acesso e regras de filtragem;

4.2.1.11.7 Possuir mecanismo que permita a realização de cópias de segurança (backups) e sua posterior restauração remotamente, através da interface gráfica, sem necessidade de se reinicializar o sistema;

4.2.1.11.8 Possuir mecanismo para possibilitar a aplicação de correções e atualizações para o firewall remotamente através da interface gráfica;

4.2.1.11.9 Permitir a visualização em tempo real de todas as conexões TCP e sessões UDP que se encontrem ativas através do firewall e a remoção de qualquer uma destas sessões ou conexões;

4.2.1.11.10 Permitir a geração de gráficos em tempo real, representando os serviços mais utilizados e as máquinas mais acessadas em um dado momento;

4.2.1.11.11 Permitir a visualização de estatísticas do uso de CPU, memória da máquina onde o firewall está rodando e tráfego de rede em todas as interfaces do Firewall através da interface gráfica remota, em tempo real e em forma tabular e gráfica;

4.2.1.11.12 Permitir a conexão simultânea de vários administradores, sendo um deles com poderes de alteração de configurações e os demais apenas de visualização das mesmas. Permitir que o segundo ao se conectar possa enviar uma mensagem ao primeiro através da interface de administração;

4.2.1.11.13 Possibilitar o registro de toda a comunicação realizada através do firewall, e de todas as tentativas de abertura de sessões ou conexões que forem recusadas pelo mesmo;

4.2.1.11.14 Possuir interface orientada a linha de comando para a administração do firewall a partir do console ou conexão SSH, sendo esta com múltiplas sessões simultâneas;

4.2.1.11.15 Possuir mecanismo que permita inspecionar o tráfego de rede em tempo real (sniffer) via interface gráfica, podendo opcionalmente exportar os dados visualizados para arquivo formato PCAP e permitindo a filtragem dos pacotes por protocolo, endereço IP origem e/ou destino e porta IP origem e/ou destino, usando uma linguagem textual;

4.2.1.11.16 Permitir a visualização do tráfego de rede em tempo real tanto nas interfaces de rede do Firewall quando nos pontos internos do mesmo: anterior e posterior à filtragem de pacotes, onde o efeito do NAT (tradução de endereços) é eliminado;

4.2.1.11.17 Possuir sistema de respostas automáticas que possibilite alertar imediatamente o administrador através de e-mails, janelas de alerta na interface gráfica, execução de programas e envio de Traps SNMP.

4.2.1.12 Requisitos de Proteção Multicamadas Contra Ameaças Avançadas em Mensagens:

4.2.1.12.1 Os requisitos mínimos exigidos neste subitem são justificados pela necessidade de proteger o ambiente de ataques dos tipos “SPAM” e “phishing”, através da inspeção avançada de mensagens eletrônicas, protegendo a rede e as caixas de correio do Estado de ataques virtuais disfarçados em mensagens de correio eletrônico, que podem ocasionar na perda de informação crítica, roubo de dados sigilosos, degradação de serviços, falta de espaço de armazenamento por conta do excesso de mensagens ou interrupção de funcionamento de sistemas de informações e equipamentos essenciais para continuidade dos serviços públicos prestados, sendo que estas especificações constituem requisitos usuais e padrão de mercado para tecnologias com esta finalidade;

4.2.1.12.2 A funcionalidade em questão deverá ser fornecida no mesmo appliance das demais funções anteriormente descritas, ou ainda em appliance adicional, “appliance virtual” ou solução em nuvem fornecida pela Contratada;

4.2.1.12.3 Em todos os casos, a funcionalidade deverá ser do mesmo fabricante, por questões de compatibilidade com as demais funções interdependentes e possibilidade de gerenciamento e monitoramento contínuo e integrado;

4.2.1.12.4 Especificações de Software:

4.2.1.12.4.1 Ser um MTA completo com suporte ao protocolo SMTP;

4.2.1.12.4.2 Possuir filtros de reputação;

4.2.1.12.4.3 Possuir solução antispam integrada;

4.2.1.12.4.4 Possuir solução antiphishing integrada;

4.2.1.12.4.5 Efetuar varredura de conteúdo (na entrada e na saída do correio eletrônico);

4.2.1.12.4.6 Possuir módulo de consulta customizada e impressão de relatórios estatísticos;

4.2.1.12.4.7 Possuir a funcionalidade de SPF;

4.2.1.12.4.8 Possuir a funcionalidade de DKIM;

4.2.1.12.4.9 Possuir a funcionalidade de DMARC.

4.2.1.12.5 Interface de Administrador:

4.2.1.12.5.1 Todos os requisitos descritos no item deverão ser consolidados em interfaces gráficas e de textos;

4.2.1.12.5.2 A interface gráfica deverá permitir acesso via HTTPS;

4.2.1.12.5.3 A mesma interface deverá gerenciar todos os produtos instalados no appliance ou virtual appliance;

4.2.1.12.5.4 A solução não pode ser intrusiva, devendo ser instalada facilmente sem modificar a estrutura da rede DMZ;

4.2.1.12.5.5 A solução deverá possuir a capacidade de criação e gerenciamento de múltiplos grupos de usuários e a definição de regras e políticas diferenciadas para cada um destes grupos.

4.2.1.12.6 Especificações do MTA:

4.2.1.12.6.1 A solução Contratada deverá possuir um software MTA focado em prover segurança, desempenho e alta disponibilidade;

4.2.1.12.6.2 O MTA deverá suportar filtros de conexões, que deverão ser executados antes que mensagens entrem no sistema, ou seja, antes do início do SMTP. Esses filtros deverão possuir a capacidade de classificar diferentes tipos de comportamento (como whitelist, blacklist e gargalos). Os filtros de conexões deverão ser configuráveis, no mínimo, por: Endereço de IP, Faixa de endereços de IP;

4.2.1.12.6.2.1 Deverão suportar RBL (listagem baseada em DNS);

4.2.1.12.6.2.2 Deverão possuir e utilizar filtros de reputação;

4.2.1.12.6.2.3 Deverão possuir a capacidade de definição das seguintes políticas: Limite de número de destinatários por mensagem, Limite do tamanho das mensagens, permitir a utilização ou não de SSL/TLS para conexão, Utilização de antispam.

4.2.1.12.6.3 Deverá suportar SSL/TLS para conexões de entrada e saída;

4.2.1.12.6.4 Deverá ser capaz de utilizar DNS reverso nas conexões de entrada;

4.2.1.12.6.5 Deverá ser capaz de processar o seguinte tráfego de mensagens:

4.2.1.12.6.5.1 Deverá suportar tráfego de entrada: aproximadamente 100.000 mensagens por dia;

4.2.1.12.6.5.2 Deverá suportar tráfego de saída: aproximadamente 100.000 mensagens por dia.

4.2.1.12.6.6 Deverá suportar, no mínimo, 30.000 (trinta mil) mailboxes;

4.2.1.12.6.7 Deverá suportar vários domínios (registros MX), e suportar roteamento de mensagens baseado em cada um desses domínios;

4.2.1.12.6.8 As filas de entrega do MTA deverão possuir tamanho suficiente para suportar uma sobrecarga de mensagens no evento de uma falha ou de um problema em outros pontos de infraestrutura de correio;

4.2.1.12.6.9 Deverá permitir o gerenciamento das filas de mensagens (queues), visualizando-as e com as opções de parar e iniciar as filas e de excluir (flush) mensagens;

4.2.1.12.6.10 Deverá suportar "aliasing";

4.2.1.12.6.11 Deverá suportar perfis únicos que tratam do comportamento de mensagens de volta (bounce) baseados nos domínios ou endereços IP de destino;

4.2.1.12.6.12 Deverá possuir “Message Tracking” na própria console gráfica para uma visualização detalhada do status da mensagem;

4.2.1.12.6.13 Deverá suportar várias quarentenas residentes no próprio "appliance ou virtual appliance", onde as mensagens deverão ser armazenadas pelo período de tempo especificado pelo administrador;

4.2.1.12.6.14 O módulo de quarentena deverá ser capaz de enviar uma notificação periódica para os usuários, informando as mensagens consideradas como SPAM que foram inseridas na quarentena;

4.2.1.12.6.15 Deverá possuir a funcionalidade de dividir mensagens baseado em políticas definidas para cada: domínio, subdomínio, grupo de usuário, usuário individual, de forma integrada com ferramentas de LDAP, AD, etc;

4.2.1.12.6.16 Deverá permitir a criação de políticas de antispam, filtros de conteúdo para cada um dos grupos criados;

4.2.1.12.6.17 Deverá permitir a criação de políticas, por usuários ou grupos, baseadas no tamanho ou tipo de anexo das mensagens.

4.2.1.12.7 Especificações dos filtros de reputação:

4.2.1.12.7.1 A solução Contratada deverá possuir um sistema que permita estabelecer uma reputação (pontuação) dos endereços IP de servidores que estarão iniciando conexões TCP. Após estabelecida essa reputação, a solução deverá permitir ações diferenciadas de acordo com a pontuação obtida;

4.2.1.12.7.2 O sistema de verificação de reputação não deverá basear-se somente em RBL´s públicas;

4.2.1.12.7.3 Esse sistema de reputação deverá utilizar uma conexão com base web nacional ou mundial, constantemente abastecida, por sua vez, de dados de várias fontes (black lists, outros appliance ou virtual appliances do mesmo fabricante implementados em outras organizações, etc.) – essa característica objetiva aumentar a precisão da pontuação fornecida;

4.2.1.12.7.4 O administrador deverá ter a possibilidade de aplicar políticas através dessa pontuação, podendo no mínimo, varrer por spam ou definir um tipo de proteção contra ameaças.

4.2.1.12.8 Especificações do software antispam:

4.2.1.12.8.1 Deverá possuir um sistema de regras que será atualizado automaticamente, numa frequência configurada pelo administrador;

4.2.1.12.8.2 Deverá possuir a possibilidade de ser configurada para analisar mensagens na entrada e na saída;

4.2.1.12.8.3 Filtrar mensagens baseadas na reputação das URLs inseridas em seu conteúdo;

4.2.1.12.8.4 Atualização automática dos filtros sem interrupção dos serviços e/ou perda das regras pré-estabelecidas pelo administrador;

4.2.1.12.8.5 Bloqueio de servidores spammers através da metodologia conhecida por Domain Keys Identified Mail (DKIM);

4.2.1.12.8.6 Ter a possibilidade de fazer approved list para domínios em se habilitando o domain keys identified mail (DKIM);

4.2.1.12.8.7 Possuir a detecção de SPAMs utilizando tecnologia heurística, podendo ser configurada a sensibilidade da ferramenta;

4.2.1.12.8.8 Permitir a criação de White e Black Lists para um melhor ajuste na detecção de SPAMs;

4.2.1.12.8.9 Permitir a proteção contra phishings;

4.2.1.12.8.10 Permitir verificar a reputação de links que estejam dentro do corpo das mensagens;

4.2.1.12.8.11 Ajuste do nível de sensibilidade do bloqueio de mensagens que tiverem links com má reputação;

4.2.1.12.8.12 Possibilidade de White List para a checagem de reputação em URLs dentro de mensagens;

4.2.1.12.8.13 Possibilidade de se verificar o hash das mensagens em tempo real para proteção contra SPAMs;

4.2.1.12.8.14 Filtros de Conteúdo contra spam deverão varrer todas as partes das mensagens, inclusive: Emissores (comando SMTP MAIL FROM), Destinatários (comando SMTP RCPT TO), Cabeçalho do e-mail, Corpo do e-mail, Anexo(s) do e-mail;

4.2.1.12.8.15 O sistema de filtros deverá suportar dicionários de palavras e expressões regulares;

4.2.1.12.8.16 O suporte de anexos deverá possuir no mínimo: Escaneamento por tipo MIME, Escaneamento por anexos compactados em pelo menos 5 (cinco) vezes, A capacidade de apagar automaticamente anexos, A capacidade de tomar decisões baseadas no tamanho de mensagem (corpo ou anexos);

4.2.1.12.8.17 Políticas baseadas na varredura deverão incluir pelo menos: Entrega da mensagem, Retorno da mensagem (bounce), Descarte da mensagem, Manipulação de cabeçalhos da mensagem, Envio de mensagem de notificação para um outro endereço, Envio de mensagem para quarentena;

4.2.1.12.8.18 As políticas deverão possuir capacidade de ser aplicadas usando as diretivas de grupo do Active Directory;

4.2.1.12.8.19 Os filtros de conteúdo deverão possuir capacidade de ser configurados para mensagens de e e-mail na entrada e na saída;

4.2.1.12.8.20 O sistema deverá possuir capacidade para efetuar varredura de byte duplo (UTF, por exemplo) para a busca em vários idiomas.

4.2.1.12.9 Especificações de Segurança do MTA:

4.2.1.12.9.1 Proteção contra Coleta do Diretório: a solução deverá possuir uma proteção contra esse tipo de ataque através da verificação integrada com LDAP, AD dos destinatários de mensagens;

4.2.1.12.9.2 Defesa contra ataque de Negação de Serviço: o sistema operacional do "appliance ou virtual appliance" deverá possuir a capacidade de identificar e proteger o MTA contra ataques por DoS;

4.2.1.12.9.3 O sistema de autenticação deverá possuir proteção contra ataques (por exemplo, coleta de usuário/senha);

4.2.1.12.9.4 Possuir recurso de firewall de e-mail, protegendo o servidor de correio contra ataques de diretório (Directory Harvest Attack);

4.2.1.12.9.5 Possuir recurso de firewall de e-mail, capaz de deferir a conexão SMTP caso a fonte emissora tenha enviado uma quantidade de mensagens consideradas como SPAM, em um determinado espaço de tempo, ambos configuráveis pelo administrador;

4.2.1.12.9.6 O appliance ou virtual appliance deverá permitir configuração de SSL/TLS;

4.2.1.12.9.7 A solução deverá ser integrada ao Active Directory da Contratante.

4.2.1.12.10 Especificações de Filtros de Segurança:

4.2.1.12.10.1 Possuir mecanismos para identificação no conteúdo das mensagens de itens como: número de cartão de crédito, RG e/ou CPF;

4.2.1.12.10.2 Possuir mecanismos para criação de diretórios de palavras pertencentes a temas específicos como, por exemplo, ofensas;

4.2.1.12.10.3 Permitir a verificação heurística contra vírus recém-lançados, mesmo sem uma vacina disponível;

4.2.1.12.10.4 Permitir a verificação do tipo real do arquivo, mesmo que o mesmo for renomeado;

4.2.1.12.10.5 Permitir que arquivos suspeitos sejam enviados ao fabricante sem intervenção do administrador;

4.2.1.12.10.6 Permitir o escaneamento de arquivos executáveis comprimidos em tempo real;

4.2.1.12.10.7 Proteção contra Spywares, sem a necessidade de um software ou agente adicional;

4.2.1.12.10.8 Proteção contra Dialers, sem a necessidade de um software ou agente adicional;

4.2.1.12.10.9 Proteção contra Ferramentas Hackers, sem a necessidade de um software ou agente adicional;

4.2.1.12.10.10 Proteção contra Ferramentas para descobrir senhas de aplicativos, sem a necessidade de um software ou agente adicional;

4.2.1.12.10.11 Proteção contra Adwares, sem a necessidade de um software ou agente adicional;

4.2.1.12.10.12 Proteção contra Ferramentas, sem a necessidade de um software ou agente adicional;

4.2.1.12.10.13 Bloqueio de malware empacotado (packed malware) de forma heurística.

4.2.1.12.11 Especificações de Atualização e Administração do MTA:

4.2.1.12.11.1 O appliance ou virtual appliance deverá fornecer atualizações através de interface web e permitir prazo máximo de espera automática para realização de atualização;

4.2.1.12.11.2 A solução deve gerar relatórios automatizados, contendo, pelo menos: sumário de mensagens, tamanho médio de mensagem, principais remetentes, por domínio e por endereço de e-mail, principais destinatários, por domínio e por endereço de e-mail, principais remetentes de SPAM, por domínio e por endereço de e-mail, principais destinatários de SPAM, por domínio e por endereço de e-mail, estatísticas sobre a quarentena, principais fontes de ataques de diretório, principais fontes de ataques de spam;

4.2.1.12.11.3 Possibilidade de agendamento e envio dos relatórios por e-mail;

4.2.1.12.11.4 Os relatórios deverão suportar pelo menos os formatos HTML e CSV;

4.2.1.12.11.5 A solução deverá fornecer relatórios de volume de mensagens entre fontes e destinos;

4.2.1.12.11.6 A solução deverá fornecer uma interface gráfica com volumes em tempo real;

4.2.1.12.11.7 Recursos adicionais parametrizáveis do appliance ou virtual appliance: Permitir configuração de fuso horário, suportar configuração manual de horário, sincronizar via Network Time Protocol (NTP);

4.2.1.12.11.8 Possuir um sistema de alertas configurável pelo administrador, fornecer, pelo menos, avisos sobre eventos críticos no sistema (falha de hardware, falta de espaço nos discos e notificação de ataque);

4.2.1.12.11.9 Possuir suporte para integração de SNMP (Simple Network Management Protocol);

4.2.1.12.11.10 Integração com serviço de diretório: Deverá integrar com vários fornecedores de serviços de diretório, dentre eles: LDAP (Lightweight Directory Access Protocol), AD (MS Active Directory);

4.2.1.12.11.11 Deverá integrar de forma anônima (sem senha) ou com usuário/senha, com suporte a conexões via SSL/TLS;

4.2.1.12.11.12 Possuir logs com um alto nível de detalhes (endereços IP e e-mail de origem e destino, reputação da origem, data, hora e políticas aplicadas); disponibilizados para acesso externo (FTP ou outro método); suportar modelo de envio (enviar logs para um servidor em horário pré-definido) e recebimento (um servidor de aplicação pode obter os logs) dos seus arquivos de “log”;

4.2.1.12.11.13 O "appliance ou virtual appliance" deverá possuir/permitir acesso remoto seguro para que o fabricante possa solucionar situações críticas via suporte remoto;

4.2.1.12.11.14 Administração via console de gerenciamento: Atualizar automaticamente os filtros, sem interrupção dos serviços;

4.2.1.12.11.15 Possuir console de administração interna ao produto, Web, sem necessidade de instalar clientes ou partes da solução em máquinas adicionais para a administração e, no caso de administração em appliance ou virtual appliance adicional, todo o hardware adicional deverá ser fornecido;

4.2.1.12.11.16 Gerenciamento via console web HTTPS (Internet Explorer / Chrome / Firefox);

4.2.1.12.11.17 A solução deve possuir um passo a passo de instalação e configuração;

4.2.1.12.11.18 Realizar atualização de forma automática das vacinas de forma incremental e da versão do software. A atualização deve permitir conexão através de serviço Proxy;

4.2.1.12.11.19 Possuir autenticação via TLS (Transport Layer Security);

4.2.1.12.11.20 Ter gerencia de área exclusiva para quarentena ou cópia de mensagens;

4.2.1.12.11.21 A interface de administração deverá possuir acesso criptografado (HTTPS ou através de software de gerenciamento, do mesmo fabricante do appliance ou virtual appliance, com diversos níveis de privilégio. Os tipos mínimos serão “administração”, “relatórios”, “quarentena” e “apenas leitura”;

4.2.1.12.11.22 Possuir quarentena por usuário proprietária do mesmo fabricante desenvolvedor da tecnologia de anti-spam fornecida, possibilitando ao usuário administrar sua própria quarentena, removendo mensagens ou liberando as que não considera SPAM, diminuindo a responsabilidade do administrador e também a possibilidade de bloqueio de e-mails legítimos. A Quarentena pode ser implementada com integração direta em aplicações de correio eletrônico, ou via interface Web (HTTPS);

4.2.1.12.11.23 Capacidade de apresentar uma console web para que os usuários possam verificar as mensagens que estejam em quarentena por motivo de spam;

4.2.1.12.11.24 Capacidade de usuários criarem lista de exceções a remetentes nessa console web de quarentena de mensagens;

4.2.1.12.11.25 Permitir que os usuários verifiquem mensagens suspeitas postas em quarentena e aprovar os remetentes sem intervenção do administrador;

4.2.1.12.11.26 Permitir exclusão automática das mensagens em quarentena;

4.2.1.12.11.27 Permitir que o próprio usuário crie listas brancas (de endereços confiáveis) pessoais, independente do administrador, e

de forma que estas listas brancas não interfiram nos filtros de outros usuários;

4.2.1.12.11.28 O módulo de quarentena deverá residir no próprio sistema do antispam e ser capaz de enviar uma notificação periódica para os usuários, informando as mensagens consideradas como SPAM que foram inseridas na quarentena, em língua portuguesa;

4.2.1.12.11.29 Deve efetuar remoção automática das mensagens armazenadas em quarentena de acordo com as configurações definidas pelo administrador;

4.2.1.12.11.30 Possuir funcionalidade de criação de “alias” e mascaramento de endereço;

4.2.1.12.11.31 Notificar o administrador por e-mail caso os filtros antispam não recebam atualizações por um determinado período de tempo. Será aceito, alternativamente, que o administrador seja notificado caso ocorram erros de atualização.

4.2.2 Requisitos Específicos para os Appliances dos SITES REMOTOS:

4.2.2.1 Os requisitos mínimos exigidos neste subitem são justificados pelas necessidades de: a) que cada localidade (sites remotos) possua uma solução que realize a interconexão ao Site Central (SGI), com o mínimo de recursos, capacidade e interfaces necessárias para garantir a otimização, gerenciamento e segurança do tráfego; b) contratar uma solução específica de mercado, com tecnologia construída para os fins a que se destinam, através de um processo de engenharia de qualidade, e não um produto adaptado em cima de um hardware ou software genérico, sem garantia de desempenho ou da qualidade de seus componentes; e c) garantir que o produto ofertado tenha as funcionalidades mínimas necessárias para qualquer hardware desta finalidade e que possam ser configurados de acordo com a especificidade da rede de dados WAN da SEFAZ/MS, independentemente de mudanças futuras na topologia da rede;

4.2.2.2 Deverão ser fornecidos para cada localidade descrita neste estudo, com exceção do SITE CENTRAL (SGI), um equipamento tipo appliance com todas as

funcionalidades exigidas, sem a necessidade de composição de um ou mais produtos;

4.2.2.3 O hardware e software que executem as funcionalidades de proteção de rede devem ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;

4.2.2.4 O equipamento deverá ser baseado em hardware desenvolvido com esta finalidade, ou seja, não sendo aceita soluções baseadas em plataforma PC ou equivalente;

4.2.2.5 Não serão permitidas soluções baseadas em sistemas operacionais abertos (OpenSource) como Free BSD, Debian ou mesmo Linux;

4.2.2.6 Todo o ambiente deverá ser gerenciado através de uma única interface, sem a necessidade de produtos de terceiros para compor a solução;

4.2.2.7 A solução oferecida deverá possuir no mínimo 05 (cinco) portas Giga Ethernet;

4.2.2.8 A solução oferecida deve prover administração através de interface WEB;

4.2.2.9 A solução oferecida deverá possuir capacidade de processamento de no mínimo 02 (dois) processadores;

4.2.2.10 A solução oferecida deverá possuir fonte AC com voltagem 110-220 automática;

4.2.2.11 A solução deve suportar no mínimo 300 Mbps de capacidade de vazão total;

4.2.2.12 A solução deverá suportar no mínimo 250 (duzentos e cinquenta) usuários;

4.2.2.13 A solução deve suportar no mínimo 100 Mbps de tráfego criptografado;

4.2.2.14 A solução deverá oferecer no mínimo capacidade para 1.000 (mil) de conexões simultâneas;

4.2.2.15 A solução deverá oferecer os serviços de inspeção de pacotes: Gateway Antivírus, Anti-Spyware, IPS e DPI SSL;

4.2.2.16 A solução deverá oferecer o serviço de filtro de conteúdo;

4.2.2.17 A solução oferecida deverá possui no mínimo classificação reguladora FCC Classe B e CE.

4.2.3 Requisitos de Aceleração WAN (para os SITES REMOTOS e SITE CENTRAL):

4.2.3.1 Os requisitos mínimos exigidos neste subitem são justificados pelas necessidades de: a) que cada ponto de presença (central e remoto) possua uma solução que realize a aceleração de pacotes de dados trafegados nos circuitos de rede, que é uma das funcionalidades principais que justificam a contratação em estudo; b) contratar uma solução específica de mercado, com tecnologia construída para os fins a que se destinam, através de um processo de engenharia de qualidade, e não um produto adaptado em cima de um hardware ou software genérico, sem garantia de desempenho ou da qualidade de seus componentes; e c) garantir que o produto ofertado tenha as funcionalidades e capacidades mínimas necessárias para qualquer hardware desta finalidade e que possam ser configurados de acordo com a especificidade da rede de dados WAN da SEFAZ/MS, independentemente de mudanças futuras na topologia da rede;

4.2.3.2 A solução ofertada deverá ser configurada junto à infraestrutura existente, em composição com as soluções descritas para o site central (item 2.3.2) e sites remotos (item 2.3.3), sem a necessidade de alteração de configurações utilizadas;

4.2.3.3 Caso a funcionalidade de aceleração WAN seja formada por uma solução baseada em conjunto de equipamentos ou softwares, estes deverão obrigatoriamente pertencer ao mesmo fabricante, por questões de compatibilidade de tecnologia, suporte técnico e garantia de funcionamento;

4.2.3.4 Caso a funcionalidade de aceleração WAN seja formada por uma solução de “appliance virtual”, deverá ser compatível com VMware ESX/ESXi ou Windows Hyper-V, por questões de administração centralizada e compatibilidade com as tecnologias já padronizadas no Estado;

4.2.3.5 Em se tratando de “appliance virtual”, a Contratada deverá fornecer plataforma de hardware compatível para a instalação da solução;

4.2.3.6 A solução de Otimização de Tráfego WAN (Wide Area Network) deverá ser implementada por meio de dispositivos virtuais ou físicos (appliances) específicos com, pelo menos, as funcionalidades de segurança, aceleração de

serviços Web (HTTP), aceleração TCP, configuração de classes de serviço para realização de QoS (*Quality of Service*), deduplicação e compressão de dados;

4.2.3.7 A solução deverá prover funcionalidade para aceleração de outras aplicações cujos dados trafeguem sobre o protocolo TCP, entre elas aplicações CITRIX ICA, serviços de correio eletrônico e de File Server;

4.2.3.8 A solução para o Site Central deverá oferecer no mínimo capacidade para 3.000 (três mil) conexões simultâneas;

4.2.3.9 A solução para o site remoto deverá oferecer no mínimo capacidade para 500 (quinhentas) conexões simultâneas;

4.2.3.10 Deverá ser possível a configuração de classes de serviço para realização de QoS na rede a partir dos próprios aceleradores/otimizadores, com as seguintes possibilidades:

4.2.3.10.1 Utilização do algoritmo HFSC (Hierarquical Fair Service Curves);

4.2.3.10.2 Suporte a variados tipos/filas de priorização de serviços simultaneamente;

4.2.3.10.3 Limitação de quantidade de conexões simultâneas;

4.2.3.10.4 Classificação das aplicações por endereços IP e Portas;

4.2.3.10.5 Especificação de VLAN para as regras;

4.2.3.10.6 Garantia de um mínimo de banda para uma determinada aplicação;

4.2.3.10.7 Especificação do limite máximo de banda a ser utilizada para uma determinada aplicação.

4.2.3.11 A solução deverá realizar deduplicação de dados em nível de bytes, com armazenamento em disco dos blocos de bytes aprendidos, implementando eliminação de dados redundantes retirando da WAN tráfego TCP previamente analisado e armazenado em cache substituindo por ""assinaturas"" de pequeno tamanho;

4.2.3.12 A solução deve prover cacheamento de dados, ou byte caching;

4.2.3.13 A solução deve prover cacheamento de arquivos, ou file caching;

4.2.3.14 A solução deve prover cacheamento de dados WEB (HTTP);

4.2.3.15 A solução deve prover aceleração de compartilhamento de arquivos Windows;

4.2.3.16 A solução deve prover aceleração de CIFS;

4.2.3.17 A solução deve prover aceleração de SMB assinado;

4.2.3.18 A solução deve prover otimização de protocolo;

4.2.3.19 A solução deve prover visualização de WFS;

4.2.3.20 A solução deve prover visualização de TCP;

4.2.3.21 A solução deve prover compressão de dados;

4.2.3.22 A solução deve prover diminuição de latência de rede;

4.2.3.23 A solução deve suportar SNMP e Syslog;

4.2.3.24 Deverá ser fornecido uma solução de aceleração WAN para cada unidade fazendária a ser atendida;

4.2.3.25 As unidades remotas deverão oferecer, no mínimo, as funcionalidades descritas anteriormente em conjunto também com: filtro de pacotes, antimalware, prevenção de intrusão e filtragem de conteúdo;

4.2.3.26 Para cada localidade, deverá ser instalado um No-Break para fornecimento de energia elétrica em casos de falta de fornecimento pela concessionária:

4.2.3.26.1 A capacidade do equipamento deverá ser dimensionada de acordo com a solução ofertada pela licitante;

4.2.3.26.2 Os custos de fornecimento do equipamento deverão estar incluídos na proposta.

4.2.4 Requisitos do Software de Gerenciamento

4.2.4.1 Os requisitos mínimos exigidos neste subitem são justificados pela necessidade da equipe técnica da SGI em gerenciar todo o ambiente tecnológico fornecido pela solução nos sites instalados, através de uma interface integrada e com acesso à configuração e ao monitoramento de todos os recursos e funcionalidades fornecidos, com disponibilidade de acesso local e/ou remoto;

4.2.4.2 Deverá ser fornecido em conjunto com a solução, um software de gerenciamento e geração de relatórios de todo o conjunto de equipamentos, com no mínimo as características abaixo:

4.2.4.2.1 Deverá obrigatoriamente ser do mesmo fabricante da solução, por questões de compatibilidade e garantia de funcionamento;

4.2.4.2.2 A solução deverá prover plataforma única de gerência para todos os ativos/soluções ofertados;

4.2.4.2.3 A solução deverá prover a aplicação e monitoramento de políticas múltiplas;

4.2.4.2.4 A solução deverá prover painel de visualização geral das soluções;

4.2.4.2.5 A solução deverá prover visualização de logs em tempo real;

4.2.4.2.6 A solução oferecida deve prover plataforma de geração de relatórios (integrada ou não) na solução que forneça acesso a gerencia de criação de relatórios através de interface WEB;

4.2.4.2.7 Permitir o envio dos relatórios, através de e-mail para usuários pré-definidos;

4.2.4.2.8 A solução oferecida deve prover relatórios de tráfego em tempo real bem como relatórios históricos (mínimo de 03 meses), e também relatórios onde os administradores possam identificar falhas através de troubleshooting (solução de problemas de acesso);

4.2.4.2.9 A solução deve prover também acesso a base de relatórios diretamente, independentemente se os dados já foram processados ou não pela solução;

4.2.4.2.10 A solução deve prover a funcionalidade de gerar relatórios agendados e os mesmos serem enviados automaticamente para 01 (um) ou mais endereços de e-mail;

4.2.4.2.11 A solução deverá prover a funcionalidade de emitir relatórios de modo geral ou para um usuário especifico, incluindo sua atividade através de conexões VPN;

4.2.4.2.12 A solução deverá prover funcionalidade de relatórios customizáveis, contendo no mínimo as seguintes métricas: Relatórios por tempo (dia/hora); Aplicações utilizadas; Aplicações utilizadas (por categoria); Relatórios de sites WEB acessados; Relatórios de sites WEB acessados (por categoria); Relatórios de sites WEB bloqueados; Relatórios de sites WEB bloqueados (por categoria); Relatórios de consumo de banda (total e por usuário).

4.3 REQUISITOS DE CAPACITAÇÃO:

4.3.1 Os requisitos mínimos exigidos neste subitem são justificados pela necessidade de não somente implantar a solução, porém mantê-la em funcionamento ininterrupto, provendo disponibilidade e desempenho durante toda a execução do contrato, através de equipe técnica especializada e apoio do fabricante na análise de problemas e atualização de seus produtos quanto à evolução tecnológica, correção de erros e vulnerabilidades e adaptação às mudanças de ambiente;

4.3.2 Deverá ser oferecido treinamento da solução ofertada para, no mínimo, 4 (quatro) participantes;

4.3.3 O treinamento deverá ser realizado na sede da SGI/SEFAZ ou em outro local apropriado, a ser acordado entre as partes, no município de Campo Grande/MS;

4.3.4 Deverá ser distribuído material de apoio a cada participante, que poderá ser em português (preferencialmente) ou inglês;

4.3.5 O conteúdo do treinamento deverá ser organizado em módulos, sequenciados logicamente, visando o conhecimento cumulativo, contendo, ao final de cada módulo, exercícios práticos com laboratórios para fixação;

4.3.6 A Contratada deverá prover os equipamentos que irão compor o laboratório do treinamento, que deverão ser equivalentes aos fornecidos para a SGI/SEFAZ-MS ou, quando não for possível, por equipamentos similares com as mesmas funcionalidades;

4.3.7 O instrutor deverá ministrar o treinamento em português com carga horária de, no mínimo, 20 (vinte) horas, abordando obrigatoriamente o seguinte conteúdo:

4.3.7.1 Instalação do produto;

4.3.7.2 Utilização da interface gráfica simples;

4.3.7.3 Configuração dos parâmetros básicos e gerenciamento de usuários;

4.3.7.4 Melhores práticas de utilização da solução;

4.3.7.5 Integração com ambientes de virtualização;

4.3.7.6 Criação de regras personalizadas (firewall, antivírus, VPN, IPS, MTA, QoS, Aceleração e outras essenciais para ativação das funcionalidades principais);

4.3.7.7 Criação de perfis de aceleração e otimização de rede e aplicações;

4.3.7.8 Configuração de ambiente de alta disponibilidade (cluster);

4.3.7.9 Configuração de parâmetros para balanceamento de carga de serviços;

4.3.7.10 Conceitos de monitoramento;

4.3.7.11 Processamento de tráfego SSL na solução.

4.3.8 A SGI/SEFAZ-MS poderá, a seu critério, em qualquer tempo, durante o treinamento, contestar a prestação do serviço, solicitando a troca de instrutor ou equipamentos de laboratório;

4.3.9 Caso a deficiência não possa ser sanada sem prejuízo para o andamento do treinamento, esse será suspenso pela SGI/SEFAZ-MS, devendo a Contratada agendar novo treinamento, sem ônus adicional para a Contratante.

4.4 REQUISITOS DE EXPERIÊNCIA PROFISSIONAL DA EQUIPE:

4.4.1 A licitante deverá prover suporte técnico especializado para a solução ofertada através de equipe técnica especializada e devidamente capacitada;

4.4.2 A equipe deverá ser composta por profissionais com as seguintes especialidades:

4.4.2.1 No mínimo 02 (dois) profissionais com as seguintes especialidades:

PERFIL 01 –Suporte Técnico e Manutenção	
Responsável por realizar todas as atividades relacionadas à suporte técnico e manutenção da solução ofertada, conforme as normas, padrões e diretrizes da fabricante.	
Experiência/Qualificação	***Modo de Comprovação***
Qualificação para prestar serviços de suporte técnico ou manutenção nas soluções do fabricante.	*Certificado de conclusão de capacitação fornecido pelo fabricante da solução.*
Formação	***Modo de Comprovação***
Não se aplica.	*Não se aplica.*

4.4.2.2 No mínimo 01 (um) profissional com as seguintes especialidades:

PERFIL 02 – Suporte Técnico e Monitoramento de Rede	
Responsável por monitorar os ativos e a gestão dos eventos de TI da solução ofertada, focados na administração e no monitoramento de rede e dos equipamentos que compõem a solução.	
Experiência/Qualificação	***Modo de Comprovação***
Certificação no software de monitoramento utilizado pelo NOC.	*Certificado de conclusão de capacitação fornecido por instituto credenciado.*
Formação	***Modo de Comprovação***
Não se aplica.	*Não se aplica.*

4.4.2.3 No mínimo 01 (um) profissional com as seguintes especialidades:

PERFIL 03 – Analista de gerenciamento de serviços de TI	
Responsável por estabelecer os processos que garantem organização e controle para cumprimento dos objetivos dos serviços contratados, alinhando assim a execução das atividades de TI aos processos de negócios de forma a garantir a execução contratual de forma plena.	
Experiência/Qualificação	***Modo de Comprovação***
Certificação ITIL (v3 ou superior) e Certificação ISO/IEC 20000	*Certificado de conclusão ITIL (v3 ou superior), fornecido por instituto credenciado.* *Certificado de conclusão ISO/IEC 20000, fornecido por instituto credenciado.*
Formação	***Modo de Comprovação***
Não se aplica.	*Não se aplica.*

4.4.3 No ato da assinatura do contrato a licitante vencedora do certame deverá apresentar comprovação de que os profissionais fazem parte do quadro funcional da proponente. A comprovação dar-se-á mediante um dos seguintes documentos:

4.4.3.1 Carteira de Trabalho e Previdência Social (CTPS);

4.4.3.2 Contrato de Prestação de Serviços, no caso de profissional autônomo;

4.4.3.3 Contrato Social, no caso de sócio proprietário.

4.5 REQUISITOS DE SEGURANÇA DA INFORMAÇÃO:

4.5.1 A Contratada deverá repassar para SGI/SEFAZ-MS todas as senhas para administração da solução, ficando a critério do Contratante alterá-las segundo sua conveniência;

4.5.2 A solução deverá ser provida de requisitos de segurança, como controle de acesso, autenticação com o uso de credenciais usuário e senha, registro de eventos em log de auditoria com informações suficientes para análise;

4.5.3 A contratada não poderá se utilizar da presente contratação para obter qualquer acesso não autorizado às informações da SGI/SEFAZ-MS;

4.5.4 A contratada não poderá veicular publicidade acerca do fornecimento a ser contratado, sem prévia autorização, por escrito, da SGI/SEFAZ-MS;

4.5.5 A contratada é responsável civil, penal e administrava quanto à divulgação indevida ou não autorizada de informações, realizada por ela ou por seus empregados;

4.5.6 É de responsabilidade da contratada garantir que as informações por ela obtidas em decorrência da execução desta contratação sejam mantidas em sigilo, não podendo

ser divulgadas, exceto se previamente acordado, por escrito, entre as partes contratantes;

4.5.7 O Termo de Confidencialidade deverá ser, assinado pelo representante legal da Contratada.

4.6 REQUISITOS SOCIAIS, AMBIENTAIS E CULTURAIS:

4.6.1 Durante a execução de tarefas no ambiente da Contratante, os funcionários da empresa fornecedora deverão observar, no trato com os servidores e o público em geral, a urbanidade e os bons costumes de comportamento, tais como: asseio, pontualidade, cooperação, respeito mútuo, discrição e zelo com o patrimônio público. Deverão ainda portar identificação pessoal, de acordo com as normas internas das instituições;

4.6.2 Todas as interfaces de operação da solução e a documentação técnica devem estar no idioma português brasileiro (preferencialmente) ou inglês;

4.6.3 A Contratada fica responsável pela destinação segura, dentro das normas ambientais, de componentes substituídos ou resíduos descartados no processo de manutenção dos equipamentos;

4.6.4 É dever da Contratada observar entre outras: o menor impacto sobre recursos naturais como flora, fauna, ar, solo e água; preferência para materiais, tecnologias e matérias-primas de origem local; maior eficiência na utilização de recursos naturais como água e energia; maior geração de empregos, preferencialmente com mão de obra local; maior vida útil e menor custo de manutenção do bem; uso de inovações que reduzam a pressão sobre recursos naturais; e origem ambientalmente regular dos recursos naturais utilizados nos bens e serviços.

5. OBRIGAÇÕES DA CONTRATANTE

5.1 Constituem obrigações da Contratante, além das demais previstas no Edital e seus Anexos ou deles decorrentes:

5.1.1 Nomeação de gestor e fiscal do contrato para acompanhar e fiscalizar a execução dos contratos;

5.1.2 Definir o controle da classificação e mensuração das ordens de serviço, quando aplicável, não sendo permitida delegação à empresa que presta os serviços mensurados;

5.1.3 Receber o objeto fornecido pela contratada que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;

5.1.4 Aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis, comunicando ao órgão gerenciador da Ata de Registro de Preços, quando aplicável;

5.1.5 Comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC;

5.1.6 Prever que os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados, pertençam à Administração;

5.1.7 Prestar as informações e os esclarecimentos que venham a ser solicitados pela CONTRATADA;

5.1.8 Facultar o acesso dos técnicos da CONTRATADA às instalações nas quais esteja prevista a execução dos serviços de manutenção preventiva ou corretiva;

5.1.9 Não permitir assistência técnica, de espécie alguma, por pessoas não autorizadas pela CONTRATADA, com exceção das efetuadas por servidores e funcionários devidamente designados e orientados para este fim.

6. OBRIGAÇÕES DA CONTRATADA

6.1 Constituem obrigações da Contratada, além das demais previstas no Edital e seus Anexos ou deles decorrentes:

6.1.1 Qualquer ato que implique a substituição do Contratado por outra pessoa jurídica, como a fusão, cisão ou incorporação, somente será admitida mediante expresso e prévio consentimento da Contratante, mediante a formalização de Termo Aditivo, desde que:

6.1.1.1 seja mantida a condição de microempresa ou empresa de pequeno porte (quando for o caso);

6.1.1.2 sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação;

6.1.1.3 sejam mantidas as demais cláusulas e condições do contrato; e

6.1.1.4 não haja qualquer prejuízo à boa execução das obrigações pactuadas.

6.1.2 Entregar os objetos ofertados, no prazo proposto e em conformidade com as especificações exigidas no Edital e seus Anexos;

6.1.3 Somente divulgar informações acerca dos objetos do contrato, que envolva o nome da contratante, mediante sua prévia e expressa autorização;

6.1.4 Manter durante a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

6.1.5 Cumprir todas as leis e posturas federais, estaduais e municipais pertinentes e responsabilizar-se por todos prejuízos decorrentes de infrações a que houver dado causa;

6.1.6 Assumir com exclusividade todos os impostos e taxas que forem devidos em decorrência do objeto do contrato, bem como as contribuições devidas à Previdência Social, encargos trabalhistas, prêmios de seguro e de acidentes de trabalho e quaisquer outras despesas que se fizerem necessárias ao cumprimento do objeto pactuado, inclusive quanto ao transporte interno dos bens;

6.1.7 Aceitar nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem, no objeto, até 25% (vinte e cinco por cento) do valor inicial atualizado do contrato;

6.1.8 Responder perante a Contratante e terceiros por eventuais prejuízos e danos decorrentes de sua demora ou de sua omissão, sob a sua responsabilidade ou por erro da execução deste contrato;

6.1.9 Responsabilizar-se por quaisquer ônus decorrentes de omissões ou erros na elaboração de estimativa de custos e que redundem em aumento de despesas para a Contratante;

6.1.10 Responsabilizar-se pelo ônus resultante de quaisquer ações, demandas, custos e despesas decorrentes de danos causados por culpa ou dolo de seus empregados, prepostos e/ou contratados, bem como se obrigar por quaisquer responsabilidades

decorrentes de ações judiciais que lhe venham a ser atribuída por força de lei, relacionadas com o cumprimento do Contrato;

6.1.11 Responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com os arts. 12, 13 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990);

6.1.12 Ceder ao Contratante os direitos de propriedade intelectual e direitos autorais da Solução de Tecnologia da Informação e Comunicação sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados;

6.1.13 Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;

6.1.14 Quando especificada, manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução de TIC;

6.1.15 Quando especificado, manter a produtividade ou a capacidade mínima de fornecimento da solução de TIC durante a execução do contrato;

6.1.16 Indicar preposto para representa-la durante a execução do contrato, com poderes de gerência local, com a missão de garantir a adequada execução do contrato, ministrar orientação aos executantes dos serviços e fiscalizar o cumprimento de suas orientações. O preposto será responsável por:

6.1.16.1 Garantir o cumprimento das atividades de acordo com as diretrizes estabelecidas para sua realização, bem como supervisionar a instalação dos equipamentos, manutenções e monitoramentos;

6.1.16.2 Reportar-se sempre ao gestor do contrato, adotando as providências pertinentes para a correção das falhas detectadas;

6.1.16.3 Receber as observações do gestor do contrato relativamente à execução do serviço e identificar as necessidades de treinamento quando constatado manuseio incorreto dos equipamentos;

6.1.16.4 Tomar as providências pertinentes para que sejam corrigidas todas as falhas detectadas e, quando houver necessidade, reportar-se ao responsável pela fiscalização designado pela Contratante, solicitando as providências que se

fizerem necessárias ao bom cumprimento de suas obrigações, recebendo as reclamações daquele e, por consequência, tomando todas as medidas cabíveis para solução das falhas detectadas;

6.1.16.5 Cumprir horários e periodicidade para a execução dos serviços fixados pela Contratante, segundo suas conveniências e em consonância com a fiscalização do contrato;

6.1.16.6 Comunicar à Contratante quaisquer fatos ou circunstâncias detectadas, quando da execução dos serviços contratados, que prejudiquem ou possam prejudicar a qualidade dos serviços objeto deste termo de referência.

6.1.17 Arcar com as despesas de transporte aéreo e terrestre, hospedagem e alimentação dos profissionais envolvidos nos serviços contratados;

6.1.18 Utilizar profissionais devidamente capacitados e habilitados para os serviços contratados, impondo-lhes rigoroso padrão de qualidade, segurança e eficiência, correndo por sua conta todas as despesas com salários, impostos, contribuições previdenciárias, encargos trabalhistas, seguros e outras correlatas;

6.1.19 Manter sigilo absoluto sobre todas as informações provenientes dos serviços realizados;

6.1.20 Realizar as atividades de manutenção e tomar todas as providências cabíveis para rápida e efetiva eliminação de falhas reclamadas, sem limite de chamados mensais;

6.1.21 Refazer serviços mal executados, completar falhas e omissões e inconformidades de qualquer natureza, sem ônus para a Contratante;

6.1.22 Afastar da prestação de serviços os empregados que possuam tenham conduta técnica ou pessoal inaceitável;

6.1.23 Responsabilizar-se por erros ou imperícias praticadas na execução dos serviços;

6.1.24 Responsabilizar-se totalmente pela observância de Leis, Regulamentos e Posturas em vigor.

7. SUBCONTRATAÇÃO

7.1 Não será admitida a subcontratação ou a formação de consórcios para fornecimento do objeto, visto que a estrutura da solução é única, não cabendo tal formação para fornecimento de objeto uno e indivisível.

8. MODELO DE EXECUÇÃO DO CONTRATO

8.1 CONDIÇÕES DE ENTREGA:

8.1.1 Diagrama Proposto:

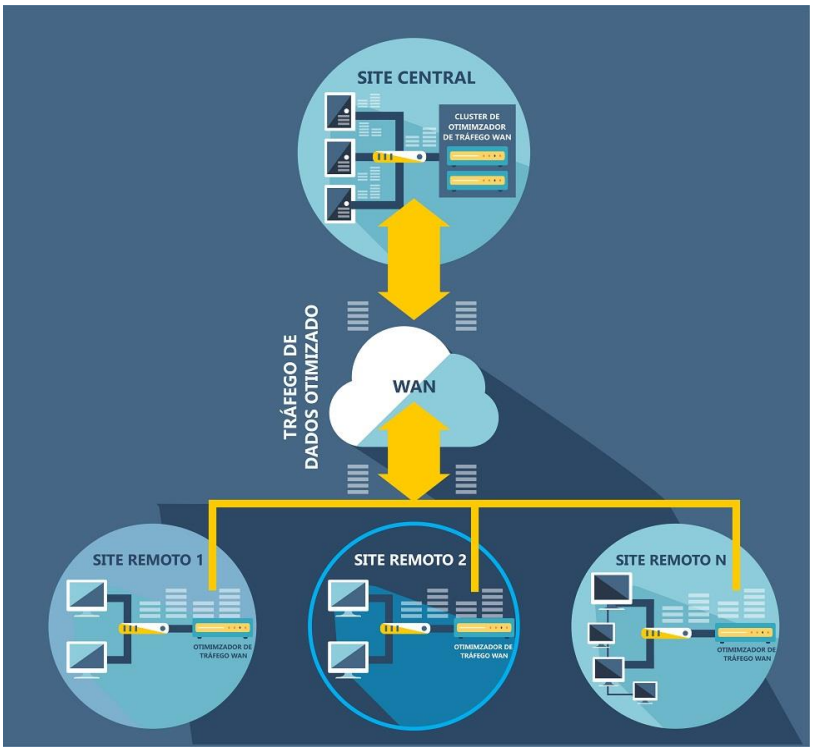

Figura 1 - Diagrama da Solução de Otimização de Tráfego WAN

8.1.2 Localidades Atendidas:

8.1.2.1 SITE CENTRAL

Id	Unidade	Endereço	Cidade
1	Superintendência de Gestão da Informação – SGI/SEFAZ	Rua Delegado Osmar de Camargo, s/n	Campo Grande

8.1.2.2 SITES REMOTOS

Id	Unidade	Endereço	Cidade
1	Agência Fazendária de Água Clara	Av. Julio Maia n. 1182 - Centro	Agua Clara
2	Agência Fazendária de Amambai	Av. Pedro Manvailer n. 3147 - Centro	Amambai
3	Posto de Atendimento de Anaurilândia	Rua Brasil, 903 - Anexo ao Iagro	Anaurilândia
4	Posto Fiscal Ofaie	Rod. MS 480 km 01	Anaurilândia
5	Agência Fazendária de Aparecida do Taboado	Rua Francisco de Queiroz n. 1823 - Jardim Jerusa	Aparecida do Taboado
6	Posto Fiscal Itamarati	Rod. MS 158 / BR prolongamento 158 - km 09	Aparecida do Taboado
7	Agência Fazendária de Aquidauana Setor de Fiscalização Regional Norte	Rua Coronel Estevão Alves Correa, n. 597 - Centro	Aquidauana

8	Posto de Atendimento de Bandeirantes	Rua Arthur Bernardes, s/n	Bandeirantes
9	Agência Fazendária de Bataguassu	Avenida Dias Barroso nº 390	Bataguassu
10	Posto Fiscal XV de Novembro	Rod. BR 267 - km 12,5	Bataguassu
11	Agência Fazendária de Bela Vista	Rua Antônio João, 675 - Centro	Bela Vista
12	Posto de Atendimento de Bonito	Rua Dr. Conrado, n. 766 - Vila Donária	Bonito
13	Posto de Atendimento de Brasilândia	Rua Raimundo Assis de Alencar n. 1021	Brasilândia
14	Posto Fiscal João André	BR 158, km 342	Brasilândia
15	Agência Fazendária de Camapuã	Rua Cuiabá n. 256 – Térreo	Camapuã
16	Coordenadoria de Logistica e Apoio Operacional	Rua 13 de maio n. 3922 - Bairro São Francisco	Campo Grande
17	Posto de Atendimento Acrissul	Rua Américo Carlos da Costa n. 296 – Parque Laucidio Coelho	Campo Grande
18	Posto Fiscal Aeroporto de Campo Grande	Av. Duque de Caxias, S/N	Campo Grande
19	Posto Fiscal Correios I	Rua Barão do Rio Branco, 555	Campo Grande
20	Posto Fiscal Correios II	Avenida Calógeras, 178	Campo Grande
21	Prático Aero Rancho	Av. Marechal Deodoro n. 2603	Campo Grande
22	Prático Bosque dos Ipês	Av. Cônsul Assaf Trad, n. 4796 - Parque Novos Estados	Campo Grande
23	Prático General Osório	Rua Santo Ângelo, 51 - Cel. Antonino	Campo Grande
24	Prático Guaicurus	Av. Guri Marques n. 5111	Campo Grande
25	Base de Fiscalização Móvel Aporé	Av. Juraci Lucas, 21 - Rod MS 306 - Área Urbana	Cassilândia
26	Posto de Atendimento de Cassilândia	Rua Antonio Batista de Almeida n. 78 - Bairro Bom Jesus	Cassilândia
27	Agência Fazendária de Chapadão do Sul	Av. Dezesseis n. 941- Centro	Chapadão do Sul
28	Base de Fiscalização Móvel Campo Bom	BR 060 - Km 01 - Divisa Goiás	Chapadão do Sul
29	Agência Fazendária de Corumbá Setor de Fiscalização Regonal Norte Setor Transportadora de Corumbá	Rua XV de Novembro, 32 – Centro	Corumbá
30	Base de Fiscalização Móvel Lampião Acesso	Rod BR 262 - KM 772	Corumbá
31	Agência Fazendária de Costa Rica	Rua José Pereira da Silva n. 659 - Centro	Costa Rica
32	Agência Fazendária de Coxim	Rua Senador Filinto Muller nº 514, Centro	Coxim
33	Posto de Atendimento de Dois Irmãos do Buriti	Av. Reginaldo Lemes da Silva n. 02 - Centro	Dois Irmãos do Buriti
34	Posto de Atendimento de Douradina	Rua João Gomes de Lira, n° 1017	Douradina

35	Agência Fazendária de Dourados Subunidade de Fiscalização de Mercadorias em Transportadoras de Dourados Subunidade de Fiscalização Externa Sul	Rua Joaquim Teixeira Alves n. 1616 - Centro Rua Antonio Emilio de Figueiredo n. 1860 - Centro Rua Onofre Pereira de Matos, n. 1640 - Centro	Dourados
36	Posto de Atendimento de Eldorado	Rua Capitão Nicolau Ritter nº 290	Eldorado
37	Agência Fazendária de Fátima do Sul	Rua Severino de Araujo, n. 1451 - Centro	Fátima do Sul
38	Posto de Atendimento Glória de Dourados	Av. Tancredo Almeida Neves s/n	Glória de Dourados
39	Posto de Atendimento de Guia Lopes da Laguna	Av. Visconde de Taunay n. 1442 - Centro	Guia Lopes da Laguna
40	Posto de Atendimento de Itaporã	Rua Fernando Correa da Costa n. 672 - Centro	Itaporã
41	Agência Fazendária de Ivinhema	Av. Panamá n. 177 - Bairro Piravevê	Ivinhema
42	Posto de Atendimento de Jaraguari	Rua Gonçalves Luiz Martins n. 410 - Centro	Jaraguari
43	Agência Fazendária de Jardim	Rua Duque de Caxias, 236 - Centro	Jardim
44	Agência Fazendária de Maracaju	Rua Waltrudes Ferreira Muzzi, s/n - Parque de Exposição	Maracaju
45	Agência Fazendária de Miranda	Praça Heróis da Laguna s/n - Bairro Beira Rio	Miranda
46	Agência Fazendária de Mundo Novo	Av. Campo Grande, 747-Centro	Mundo Novo
47	Posto Fiscal Ilha Grande	BR 163 - km 06	Mundo Novo
48	Agência Fazendária de Naviraí Setor de Fiscalização Regional Sul	Av. Campo Grande, 188 - Centro	Naviraí
49	Posto Fiscal Foz do Amambai	Rod. MS 487 - km 116	Naviraí
50	Posto de Atendimento de Nova Alvorada do Sul	Rua Irineu de Souza Araújo, 1015 - Centro	Nova Alvorada do Sul
51	Agência Fazendária de Nova Andradina	Rua Professor João de Lima Paes, n. 1145 - Centro	Nova Andradina
52	Agência Fazendária de Paranaíba Setor de Fiscalização Regional Norte Subunidade de Fiscalização de Mercadorias em Transportadoras de Paranaíba	Rua Capitão Martinho, 619 - Centro	Paranaíba
53	Posto Fiscal Alencastro	Rod. BR 497 - KM 15 - Zona Rural	Paranaíba

54	Agência Fazendária de Ponta Porã Setor de Fiscalização Regional Sul	Av. Brasil n. 3038 - Centro Rua 07 de setembro n. 311 - Centro	Ponta Porã
55	Base de Fiscalização Móvel Pacuri	Rod. BR 463, km 90	Ponta Porã
56	Agência Fazendária de Porto Murtinho	Rua Coronel Alfredo Pinto, 225- Centro	Porto Murtinho
57	Posto de Atendimento de Ribas do Rio Pardo	Rua Carlos Anconi, 1617 - Jd Vista Alegre	Ribas do Rio Pardo
58	Agência Fazendária de Rio Brilhante	Av. Lourival Barbosa n. 474	Rio Brilhante
59	Posto de Atendimento de Rio Negro	Rua Massato Masubara, 50 Centro	Rio Negro
60	Posto de Atendimento Rio Verde de Mato Grosso	Rua Vitória, n. 1131 - Centro	Rio Verde de Mato Grosso
61	Posto de Atendimento de Rochedo	Rua Albino Coimbra n. 325	Rochedo
62	Agência Fazendária São Gabriel d' Oeste	Rua Minas Gerais n. 869 - Centro	São Gabriel do Oeste
63	Posto de Atendimento de Selvíria	Av. João Selvirio de Souza, n. 636	Selviria
64	Posto Fiscal Selviria	Prolongamento Rod. MS 444 - Selvíria até a Barragem	Selvíria
65	Agência Fazendária de Sete Quedas	R. Monteiro Lobato, 628	Sete Quedas
66	Agência Fazendária de Sidrolândia	R. Minas Gerais, 620	Sidrolândia
67	Agência Fazendária de Sonora	Rua Beat Rolf Stucki, n. 22 - Centro	Sonora
68	Posto Fiscal Sonora	Rod. BR - km 163	Sonora
69	Posto de Atendimento de Terenos	Rua Professor João Egidio Zambelli n. 43 Centro	Terenos
70	Posto Fiscal Jupiá	Rod. BR 262 - km 02 (Av. Ranulpho Marques Leal n. 4040)	Três Lagoas
71	Setor de Fiscalização Regional Norte Gestoria de Fiscalização de Trânsito Norte/GFTN	Av. Antônio Trajano, 592 - Centro	Três Lagoas
72	Subunidade de Fiscalização de Mercadorias em Transportadoras de Três Lagoas Agência Fazendária de Três Lagoas Setor Transportadora de Três Lagoas	Av. Capitão Olinto Mancini n. 2462	Três Lagoas

8.2 CRITÉRIOS DE ACEITAÇÃO:

8.2.1 As soluções ofertadas deverão ser entregues diretamente nos endereços constantes nas localidades a serem atendidas;

8.2.2 As entregas nas unidades remotas deverão ser agendadas com um representante da SGI/SEFAZ para autorização de entrada nos prédios de cada unidade da SEFAZ-MS;

8.2.3 A instalação dos equipamentos e a sua colocação em funcionamento correrão por conta e responsabilidade da Contratada;

8.2.4 Todos os itens necessários à instalação da solução nas unidades remotas correrão por conta da Contratada, como cabos, conectores e demais acessórios;

8.2.5 Nas unidades remotas a solução deverá ser instalada em rack de piso ou de parede, padrão 19”, com medidas adequadas para acomodação da solução. Caso a localidade já possua um rack com medidas adequadas, este poderá ser utilizado para acomodação da solução. Caso contrário, este deverá ser providenciado pela Contratada;

8.2.6 Serão recusados os equipamentos imprestáveis ou defeituosos, que não atendam às especificações constantes neste termo de referência e/ou que não estejam adequados para o uso;

8.2.7 A Contratada deve assumir inteira responsabilidade pela devolução dos equipamentos que não estiverem de acordo com as especificações técnicas previstas neste termo de referência;

8.2.8 O recebimento do objeto não exclui a responsabilidade da Contratada pelo perfeito desempenho dos equipamentos fornecidos, cabendo-lhe sanar quaisquer irregularidades detectadas quando da utilização dos mesmos;

8.2.9 Os equipamentos deverão ser devidamente instalados nos locais determinados pela Contratante e encontrar-se em perfeito funcionamento. A instalação dos equipamentos deverá ser de acordo com as determinações da Contratante, atendendo perfeitamente às especificações e condições previstas no termo de referência;

8.2.10 A Contratada deverá atender à Contratante em eventuais mudanças da localização dos equipamentos entre os setores da Contratante;

8.2.11 Ao final do contrato, a Contratada, às suas expensas, responsabilizar-se-á pela retirada dos equipamentos instalados.

8.2.12 Prazos:

8.2.12.1 O prazo para entrega da solução proposta será de 15 (quinze) dias corridos, contados a partir da assinatura do instrumento contratual;

8.2.12.2 O prazo para instalação e ativação da solução em ambiente de produção é de até 15 (quinze) dias corridos a partir do recebimento definitivo dos produtos;

8.2.12.3 Mensalmente, deverá ser entregue um "Relatório de Atividades Técnicas" indicando todos os eventos de suporte técnico e manutenção atendidos no período. O Relatório deverá conter no mínimo:

8.2.12.3.1 Identificação de cada chamado;

8.2.12.3.2 Identificação do tipo de atendimento;

8.2.12.3.3 Data de atendimento (abertura e conclusão);

8.2.12.3.4 Descrição do atendimento;

8.2.12.3.5 Procedimentos adotados para a solução do problema;

8.2.12.3.6 Sem prejuízo da entrega do Relatório Gerencial, a Contratante poderá solicitar, em formato digital, informações analíticas e sintéticas dos chamados técnicos abertos e fechados no período.

8.3 CONDIÇÕES DE GARANTIA E MANUTENÇÃO:

8.3.1 Os requisitos mínimos exigidos neste subitem são justificados pela necessidade de não somente implantar a solução, porém mantê-la em funcionamento ininterrupto, provendo disponibilidade e desempenho durante toda a execução do contrato, através de equipe técnica especializada e apoio do fabricante na análise de problemas e atualização de seus produtos quanto à evolução tecnológica, correção de erros e vulnerabilidades e adaptação às mudanças de ambiente;

8.3.2 Quanto ao serviço de prestação dos serviços de Suporte Técnico Especializado, reforçamos que, apesar de fundamentalmente tratar-se de outsourcing de solução de tecnologia da informação, é evidente que o suporte técnico é primordial para a manutenção da plataforma de gerenciamento, segurança e otimização de tráfego de rede WAN, conforme justificamos abaixo:

8.3.2.1 O ambiente de rede WAN a ser suportado é crítico para manutenção dos serviços públicos da SEFAZ/MS. Qualquer evento que ocasione a parada ou mal funcionamento do ambiente computacional assegurado pela tecnologia

em questão poderá causar prejuízos diretos e indiretos para o Estado, incluindo a interrupção da rede de dados das localidades atendidas, a perda ou roubo de dados críticos e/ou sigilosos, ataques de vírus, hackers e outras ameaças virtuais, e ainda a completa paralização da prestação de serviços públicos mantidos pelo ambiente de tecnologia em questão;

8.3.2.2 Considerando que as atividades desta Superintendência são realizadas ininterruptamente, não se justifica que os serviços de suporte técnico sejam prestados somente em horário comercial, bem como não haja meios digitais para que estes sejam solicitados. Ademais, o atendimento local é essencial, considerando que problemas que demandem intervenção física nas plataformas são comumente necessários;

8.3.2.3 Destacamos que o modelo de assistência local e ininterrupta não se trata de novação, sendo que é comum no mercado que as empresas que possuem produtos desta natureza, equivalentes ao esperado neste processo, prestem os serviços almejados dentro dos requisitos estabelecidos;

8.3.2.4 Não há requisitos de garantia contratual a serem considerados neste estudo, visto que os equipamentos são parte de uma solução computacional ampla (hardware, software e serviços) que serão fornecidos pela Contratada durante a vigência do contrato, e considerando que qualquer manutenção será realizada às expensas da Contratada, sem ônus adicional ao Contratante enquanto este estiver vigente, não há motivação para se exigir garantia adicional àquela já fornecida pelo fabricante, mesmo que este forneça somente pela garantia legal de 90 (noventa) dias prevista no Código de Defesa do Consumidor.

8.3.3 Tipos de serviços de suporte técnico e manutenção:

8.3.3.1 Manutenção Preventiva: Compreende visitas periódicas, conforme política definida pelo fabricante, no ambiente da Contratante (Site Central), programadas a fim de verificar a saúde do equipamento e mitigar riscos devido ao uso continuado dos serviços, incluindo:

8.3.3.1.1 Procedimentos técnicos destinados a prevenir a ocorrência de erros e defeitos de forma proativa;

8.3.3.1.2 Realização de inspeções nos equipamentos, componentes, dispositivos e softwares de configuração gerenciam a solução;

8.3.3.1.3 Verificação geral com vistas a manter sua plena funcionalidade e saúde dos equipamentos;

8.3.3.1.4 Analisar logs de sistema e sugerir mudanças para uma melhor prática de utilização da ferramenta. A equipe técnica da Contratante decidirá sobre a aplicação ou não das recomendações;

8.3.3.1.5 Sugerir, preventivamente, a aplicação de novas correções, patches, fixes, updates, service packs, novas releases, versions, builds e upgrades.

8.3.3.2 Manutenção Corretiva: Compreende visitas pontuais, a partir de abertura de chamados advindos do Contratante, a fim de atuar em incidentes ou problemas identificados que impeça o seu funcionamento regular e requeira uma intervenção técnica especializada, na localidade de instalação da solução (Central ou Remota), incluindo:

8.3.3.2.1 Reinstalação de hardwares e softwares, configuração, gerenciamento, com vistas a normalidade da operação dos serviços prestados;

8.3.3.2.2 Reparar, corrigir, remover, refazer ou substituir, no todo ou em parte, os serviços, peças ou materiais em que se verificarem imperfeições, vícios, defeitos ou incorreções, dentro dos prazos estabelecidos nos demais subitens deste estudo;

8.3.3.2.3 Corrigir defeitos de fabricação ou projeto;

8.3.3.2.4 Acondicionar adequadamente os equipamentos cujo reparo não possa ser realizado nas dependências da SGI/SEFAZ-MS, de forma a permitir sua completa segurança e identificação durante o transporte, responsabilizando-se pela sua remoção e devolução ao local em que deve ser instalado e pelas despesas operacionais decorrentes;

8.3.3.2.5 Substituir os equipamentos que apresentarem defeito de fabricação, dentro dos prazos estabelecidos;

8.3.3.2.6 Detectar problemas e limitações de desempenho da solução relacionados a softwares e/ou firmware instalados nos elementos que

fazem parte do objeto desta contratação, substituindo-os por nova versão que implemente suas correções;

8.3.3.2.7 Substituir software e/ou firmware instalados nos elementos que fazem parte do objeto desta contratação por nova versão eventualmente lançada, quando esta implementar correções a possíveis problemas ou limitações de desempenho da solução.

8.3.4 Suporte técnico especializado e manutenção prestados pela Contratada:

8.3.4.1 A Contratada deverá, de acordo com as políticas de assistência técnica do fabricante da solução, prestar os serviços de suporte técnico especializado e manutenção para toda a solução de hardware e software, para orientação de uso e administração, atualização de versões, patchs e correções de bugs, configuração e parametrização, durante toda a vigência do contrato;

8.3.4.2 O funcionamento da solução deverá ser garantido pela Contratada durante toda a vigência do contrato, que deverá se valer dos meios necessários para manter a solução operacional;

8.3.4.3 Poderão ser prestados pela empresa Contratada em ambiente on-site ou remoto, no regime 24X7, incluindo a atualização de softwares e bases de dados de conhecimento as suas expensas, e, sempre que for necessário ao bom funcionamento da solução adquirida;

8.3.4.4 Deverão ser executados por técnicos qualificados, conforme previsto nos requisitos de qualificação da equipe técnica presentes neste documento;

8.3.4.5 Quando realizados presencialmente, deverão ser prestados no endereço indicado pelo Contratante;

8.3.4.6 Todas as peças e componentes necessários ao perfeito funcionamento de toda a solução, quando necessário, devem ser substituídos pela Contratada, sem nenhum custo adicional a Contratante;

8.3.4.7 A Contratada deverá cumprir rigorosamente todos os procedimentos de manutenção definidos pela SGI/SEFAZ-MS, como horário estabelecido para parada dos equipamentos, autorizações de acesso, entre outros;

8.3.4.8 Quando a intervenção implicar interrupção da solução, mesmo que parcial, a SGI/SEFAZ-MS poderá determinar que a Contratada a execute fora do horário

de expediente do órgão, inclusive em finais de semana, sem qualquer ônus adicional a Contratante;

8.3.4.9 Fica vedada a desativação de hardware, software ou quaisquer recursos computacionais da Contratante, sem prévio conhecimento e autorização expressa da Administração;

8.3.4.10 Caso seja necessária a desativação de hardware, software ou quaisquer recursos computacionais da SGI/SEFAZ-MS, a Contratada deverá disponibilizar equipamento de redundância com capacidade igual ou superior ao que será desativado, até que o problema seja sanado, sob pena de inexecução parcial do contrato;

8.3.4.11 Em caso de retirada do equipamento, a SGI/SEFAZ-MS poderá, a seu critério, reter as unidades de memória física dos equipamentos, sem custo adicional;

8.3.4.12 Havendo necessidade de substituição de hardware (equipamentos), a Contratada deverá efetuar a substituição por mesmo modelo de peça, ou por modelo superior em características técnicas, do mesmo fabricante, sem ônus para o Contratante, quando comprovados defeitos que comprometem seu desempenho, obedecendo os critérios abaixo, sem prejuízo de outras situações que caracterizem necessidade de troca:

8.3.4.12.1 Caso ocorram 04 (quatro) ou mais defeitos que comprometam seu uso normal, dentro de qualquer intervalo de 30 (trinta) dias;

8.3.4.12.2 O equipamento (hardware) empregado em substituição ao equipamento defeituoso deverá ter os mesmos serviços de suporte técnico e manutenção durante toda a vigência restante do contrato;

8.3.4.12.3 No caso de problema recorrente no mesmo hardware, seja na restauração ou substituição das peças, em um período inferior a 2 (dois) meses, a Contratada deverá substituir o equipamento.

8.3.4.13 Quando solicitado pela SGI/SEFAZ-MS, a Contratada deverá fornecer, em até 3 (três) dias úteis, manuais, documentação de operação, documentos de troubleshooting e/ou qualquer outro tipo de documento técnico de administração, customização, operação e monitoração dos equipamentos e softwares instalados na SGI/SEFAZ-MS;

8.3.4.14 As atualizações de versões de todos os componentes da solução (major, minor, patches e fixes) deverão estar disponíveis para uso da SGI/SEFAZ-MS durante todo período contratual e sem custo adicional, podendo ser realizado download diretamente do sítio oficial do fabricante, devendo ser entregue, a última versão vigente na data do término do contrato.

8.3.5 Suporte técnico especializado e manutenção prestados pelo Fabricante:

8.3.5.1 A prestação destes serviços deve ainda contemplar o suporte técnico direto do fabricante da solução, a ser utilizado sempre que necessário, e pelo período vigente do contrato com, no mínimo, as seguintes características:

8.3.5.1.1 O suporte do fabricante deve ter um sistema de abertura de chamados para acompanhamento, 24 horas por dia e 7 dias por semana. Para atendimento telefônico, deve operar em língua portuguesa, pelo menos em regime 8x5 (oito horas por dia, sete dias por semana);

8.3.5.1.2 Deve-se assegurar a utilização de novas versões de software da solução sem ônus, sempre que esta estiver disponível;

8.3.5.1.3 Deve-se permitir o acesso à base de conhecimento da solução.

8.3.6 Sempre que solicitado pela Contratante, deve-se informar o estado do chamado aberto, por telefone da central de atendimento e/ou por sistema de controle de chamados da Contratada disponibilizado pela internet:

8.3.6.1 Caso o chamado seja repassado pela Contratada ao fabricante, o SGI/SEFAZ-MS deverá ter capacidade visualizar diretamente no sítio do fabricante o andamento desse chamado;

8.3.6.2 Deverão ser fornecidas permissões de acesso no sítio do fabricante e da Contratada para acompanhamento de chamados, download e acesso a documentação, patches, fixes, firmwares, arquivos de qualquer tipo e/ou qualquer outro material referente à solução.

8.3.7 Núcleo de Operações e Controle:

8.3.7.1 A Contratada deverá manter um NOC (Núcleo de Operações de Rede), nas dependências da Contratante, para diagnosticar preventivamente e corretivamente problemas nas soluções fornecidas e tomar as decisões de intervenção para a devida assistência técnica;

8.3.7.2 O NOC deverá ser composto por ambiente de monitoramento das soluções ofertadas, e deverá ser mantido pela Contratada em regime 8x5 (oito horas por dia, cinco dias por semana), durante a vigência do contrato, e deverá ser composto por, no mínimo, por um colaborador, devidamente certificado para a solução ofertada, para prestar o pronto-atendimento as solicitações de suporte de primeiro e segundo nível identificadas no NOC e/ou usuários finais das soluções.

8.4 PAGAMENTO

8.4.1 O pagamento, decorrente do fornecimento do objeto desta licitação, será efetuado mensalmente, mediante crédito em conta corrente, no prazo de 30 (trinta) dias do mês subsequente à execução do serviço ou entrega da parcela dos produtos, após a apresentação da respectiva nota fiscal, devidamente atestada pelo setor competente, conforme dispõe o art. 40, inciso XIV, alínea “a”, combinado com o art. 73, inciso I, alínea “b”, arts. 86, § 3º e 87, § 1º da Lei n° 8.666/93 e alterações;

8.4.2 A Contratada, durante toda a execução do contrato, deverá manter todas as condições de habilitação e qualificação exigidas na licitação;

8.4.3 Constatada a situação de irregularidade em quaisquer das certidões da Contratada, a mesma será notificada, por escrito, sem prejuízo do pagamento pelo objeto já executado, para, num prazo de 05 (cinco) dias úteis, regularizar tal situação ou, no mesmo prazo, apresentar defesa, em processo administrativo instaurado para esse fim específico;

8.4.4 O prazo para regularização ou encaminhamento de defesa de que trata o subitem anterior poderá ser prorrogado uma vez e por igual período, a critério da Contratante;

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

8.4.6 Persistindo a irregularidade, a Contratante, em decisão fundamentada, deverá aplicar a penalidade cabível nos autos do processo administrativo correspondente;

8.4.7 Não será efetuado qualquer pagamento à empresa Contratada enquanto houver pendência de liquidação da obrigação financeira em virtude de penalidade ou inadimplência contratual;

8.4.8 Na pendência de liquidação da obrigação financeira em virtude de penalidade ou inadimplência contratual o valor será descontado da fatura ou créditos existentes em favor da Contratada;

8.4.9 O documento de cobrança da CONTRATADA será a fiscal/fatura, na qual obrigatoriamente deverá constar as informações referentes ao número da conta corrente, agência e banco para depósito;

8.4.10 Caso se constate erro ou irregularidade na nota fiscal/fatura, o órgão, a seu critério, poderá devolvê-la, para as devidas correções, ou aceitá-la, com a glosa da parte que considerar indevida, nesta hipótese, o prazo para pagamento iniciar-se-á após a regularização da situação ou reapresentação do documento fiscal, não acarretando qualquer ônus para a Contratante;

8.4.11 Na hipótese de devolução, a nota fiscal/fatura será considerada como não apresentada, para fins de atendimento das condições contratuais;

8.4.12 A CONTRATANTE não pagará, sem que tenha autorização prévia e formal nenhum compromisso que lhe venha a ser cobrado diretamente por terceiros, sejam ou não instituições financeiras;

8.4.13 Os eventuais encargos financeiros, processuais e outros, decorrentes da inobservância, pela CONTRATADA de prazo de pagamento, serão de sua exclusiva responsabilidade;

8.4.14 A CONTRATANTE efetuará retenção, na fonte, dos tributos e contribuições sobre todos os pagamentos devidos à fornecedora classificada;

8.4.15 As despesas com deslocamento de pessoal da CONTRATADA ou de seus representantes serão de sua exclusividade responsabilidade.

9. MODELO DE GESTÃO DO CONTRATO

9.1 GESTÃO E FISCALIZAÇÃO:

9.1.1 Nos termos do art. 67 Lei nº 8.666, de 1993, será designado servidor ou comissão responsável pela gestão do contrato e acompanhamento e fiscalização da entrega dos bens ou serviços, anotando em registro próprio todas as ocorrências relacionadas com a execução e determinando o que for necessário à regularização de falhas ou defeitos observados;

9.1.2 O(s) responsável(eis) pela gestão e fiscalização do contrato serão designados formalmente por ato da Contratante;

9.1.3 A fiscalização de que trata este item não exclui nem reduz a responsabilidade da Contratada, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas ou vícios redibitórios, e, na ocorrência desta, não implica em corresponsabilidade da Administração ou de seus agentes e prepostos, de conformidade com o art. 70 da Lei nº 8.666/93;

9.1.4 O servidor ou comissão designada para a gestão e fiscalização do contrato anotará em registro próprio todas as ocorrências relacionadas com a execução deste, indicando dia, mês e ano, bem como o nome dos funcionários eventualmente envolvidos, determinando o que for necessário à regularização das falhas ou defeitos observados e encaminhando os apontamentos à autoridade competente para as providências cabíveis;

9.1.5 A contratada permitirá e oferecerá condições para a mais ampla e completa fiscalização, durante a vigência do contrato, fornecendo informações, propiciando o acesso à documentação pertinente e atendendo às observações e exigências apresentadas pela fiscalização;

9.1.6 A Contratada se obriga a permitir que a auditoria interna da Contratante e/ou auditoria externa por ela indicada tenha acesso a todos os documentos que digam respeito ao Contrato;

9.1.7 A Contratante realizará avaliação da qualidade do atendimento, dos resultados concretos dos esforços sugeridos pela Contratada e dos benefícios decorrentes da política de preços por ela praticada;

9.1.8 A avaliação será considerada pela Contratante para aquilatar a necessidade de solicitar à Contratada que melhore a qualidade dos produtos ofertados, para decidir sobre a conveniência de renovar ou, a qualquer tempo, rescindir o Contrato ou,

ainda, para fornecer, quando solicitado pela Contratada, declarações sobre seu desempenho, a fim de servir de prova de capacitação técnica em licitações públicas.

9.2 GESTOR E FISCAL DO CONTRATO:

9.2.1 Gestor do Contrato:

- **Nome:** Alessandro Menezes de Souza
- **Matrícula:** 427081025
- **Órgão:** Superintendência de Gestão da Informação (SGI/SEFAZ-MS)
- **e-Mail:** gabinetesgi@fazenda.ms.gov.br
- **Telefone:** (67)3318-3581

9.2.2 Fiscal do Contrato:

- **Nome:** Gustavo Nantes Gualberto
- **Matrícula:** 467284021
- **Órgão:** Superintendência de Gestão da Informação (SGI/SEFAZ-MS)
- **E-mail:** assessoriasgi@fazenda.ms.gov.br
- **Telefone:** (67) 3318-3636

9.3 ACORDOS DE NÍVEL DE SERVIÇOS:

9.3.1 Para a prestação dos serviços de suporte técnico especializado e manutenção, a Contratada deverá cumprir os tempos para resolução de chamados abertos, seguindo as seguintes premissas:

9.3.1.1 O tempo de solução será contabilizado entre a abertura do chamado e restabelecimento do sistema em sua totalidade, bem como se entende por término do reparo do equipamento a sua disponibilidade para uso em perfeitas condições de funcionamento no local onde está instalado;

9.3.1.2 O tempo de atendimento inicia-se com a primeira intervenção pelo representante da CONTRATADA, local ou remotamente;

9.3.1.3 A contratada deverá se adequar aos seguintes níveis de serviço quando ocorrerem os chamados para Suporte Técnico Especializado, Manutenção e Apoio:

MANUTENÇÃO PREVENTIVA				
Indicador	Tipo do Chamado	Inicio do atendimento	Prazo de Solução	Multa por descumprimento % em relação a fatura mensal
N01	Manutenção Programada	Data programada conforme cronograma	Período programado no chamado	1% por mês em que houver descumprimento por não atendimento, limitado a 10%.

MANUTENÇÃO CORRETIVA					
Indicador	Tipo do Chamado	Descrição	Inicio do atendimento	Prazo de Solução	Multa por descumprimento % em relação a fatura de suporte
N02	Urgente	Solução parada, no todo ou em parte, no ambiente de produção provocando uma indisponibilidade parcial ou total do ambiente de produção da Contratante durante programas de governo em período de sazonalidade.	Em até 02 (duas) horas	Em até 06 (seis) horas	2% por hora para as 4 primeiras horas que excederem o prazo; 4% por hora para as demais horas que excederem as primeiras 4 horas de descumprimento prazo.
N03	Alto Impacto	Solução parada, no todo ou em parte, no ambiente de produção provocando ao menos uma indisponibilidade parcial do ambiente de produção da Contratante.	Em até 04 (quatro) horas	Em até 12 (doze) horas	1% por hora para as 4 primeiras horas que excederem o prazo; 2% por dia que exceder o descumprimento prazo de solução.
N04	Importante	Erros ou problemas reincidentes que impactam o ambiente de produção.	Em até 08 (quatro) horas	Em até 24 (vinte e quatro) horas	1% por dia que exceder o descumprimento do prazo de solução.
N05	Normal	Problemas contornáveis que não causem lentidão ou indisponibilidade dos serviços ou aqueles para os quais houver solução de contorno.	Em até 24 (vinte e quatro) horas	Em até 2 dias	0,5% dia que exceder o descumprimento do prazo de solução.

9.3.2 Somente será admitido pedido de prorrogação dos prazos descritos na tabela de níveis de serviços mediante justificativas por escrito, plenamente fundamentadas e entregues à Contratante dentro do período correspondente ao atendimento ou resolução do chamado aberto;

9.3.3 A não resolução dos chamados dentro do prazo acima estipulado ensejará às multas e sanções previstas. Após o limite estabelecido para aplicação das multas a Contratrada deverá substituir os equipamentos conforme prazos e condições descritas abaixo, sob pena de incorrer em inexecução total do contrato;

9.3.4 Se o atendimento classificado como URGENTE não for resolvido dentro do prazo estabelecido, mesmo após a execução dos serviços de reparo (atualização de softwares/substituição de peças de hardware), o equipamento deverá ser integralmente substituído no prazo máximo de 02 (dois) dias, segundo as características técnicas e de desempenho iguais ou superiores ao bem anterior de modo que não cause nenhum impacto no serviço sustentado pelos equipamentos, sem ônus para a Contratante, sob pena de caracterizar inexecução parcial do contrato;

9.3.5 Se o problema identificado como ALTO IMPACTO persistir pós-atendimento técnico, e não for resolvido de forma definitiva pela empresa contratada dentro do prazo estabelecido, podendo ser prorrogado por igual período (corrido), desde que justificado, o produto deverá ser integralmente substituído no prazo máximo de 04 (quatro) dias, segundo as características técnicas e de desempenho iguais ou superiores ao bem anterior, sem ônus para a Contratante, sob pena de caracterizar inexecução parcial do contrato;

9.3.6 Se o problema identificado como IMPORTANTE persistir pós-atendimento técnico, e não for resolvido de forma definitiva pela empresa contratada dentro do prazo estabelecido, podendo ser prorrogado por igual período (corrido), desde que justificado, o produto deverá ser integralmente substituído no prazo máximo de 07 (sete) dias, segundo as características técnicas e de desempenho iguais ou superiores ao bem anterior, sem ônus para a Contratante, sob pena de caracterizar inexecução parcial do contrato;

9.3.7 Se o problema identificado como NORMAL não for resolvido de forma definitiva pela empresa contratada dentro do prazo estabelecido, podendo ser prorrogado por igual período (corrido), desde que justificado, a partir do sétimo dia, será aplicada glosa de 1% (um por cento) ao dia sobre o valor do faturamento mensal até que o problema seja integralmente sanado, limitado a 30 (trinta) dias, após esse prazo será caracterizado inexecução parcial do contrato;

9.3.8 Se após 30 (trinta) dias a contar da notificação de aplicação da multa por inexecução parcial do contrato, a Contratada não substituir os equipamentos, será

caracterizado inexecução total do contrato, sem prejuízo da continuidade do suporte técnico dos demais equipamentos em garantia;

9.3.9 A inobservância das condições aqui estabelecidas sujeitará a Contratada às penalidades previstas neste termo e no contrato.

9.4 SANÇÕES ADMINISTRATIVAS

9.4.1 Com fundamento no artigo 7° da Lei Federal n. 10.520/2002 e no artigo 50 do Decreto n. 15.327/2019, ficará impedida de licitar e contratar com o Estado do Mato Grosso do Sul e será descredenciada do Cadastro Central de Fornecedores do Estado de Mato Grosso do Sul - CCF/MS, pelo prazo de até 5 (cinco) anos, sem prejuízo da aplicação de multa de até 10% (dez por cento) sobre o valor total do item e das demais cominações legais, garantindo o direito à ampla defesa, a licitante que, convocada dentro do prazo de validade de sua proposta:

9.4.1.1 Não assinar o termo de contrato ou aceitar/retirar o instrumento equivalente, quando convocado dentro do prazo de validade da proposta;

9.4.1.2 Não entregar a documentação exigida no edital;

9.4.1.3 Apresentar documentação falsa;

9.4.1.4 Causar atraso na execução do objeto;

9.4.1.5 Não mantiver a proposta;

9.4.1.6 Falhar na execução do contrato;

9.4.1.7 Fraudar a execução do contrato;

9.4.1.8 Comportar-se de modo inidôneo;

9.4.1.9 Declarar informações falsas; e

9.4.1.10 Cometer fraude fiscal.

9.4.2 Para fins do disposto no subitem 9.4.1.8, reputar-se-ão inidôneos atos direcionados a prejudicar o bom andamento do certame, tais como a fraude ou frustração do caráter competitivo do procedimento licitatório, ação em conluio ou em desconformidade com a lei, indução deliberada a erro no julgamento, prestação falsa de informações, apresentação de documentação com informações inverídicas, ou que contenha emenda ou rasura, destinada a prejudicar a veracidade de seu

teor original, constituindo-se como exemplos as condutas tipificadas nos artigos 90, 93, 95, 96 e 97, parágrafo único, da Lei n. 8.666/1993;

9.4.3 Com fundamento nos artigos 86 e 87, incisos I a IV, da Lei n o 8.666, de 1993 e no art. 7° da Lei no 10.520, de 17/07/2002, nos casos de retardamento, de falha na execução do contrato ou de inexecução total do objeto a contratada poderá ser apenada, isoladamente ou juntamente com as multas definidas nos itens 9.4.4, 9.4.5 e 9.4.6, com as seguintes penalidades:

9.4.3.1 Advertência;

9.4.3.2 Suspensão temporária de participação em licitação e impedimento de contratar com a Administração Pública Estadual, por prazo não superior a dois anos;

9.4.3.3 Declaração de inidoneidade para licitar ou contratar com a Administração Pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a Contratada ressarcir a Administração pelos prejuízos resultantes e após decorrido o prazo da sanção aplicada com base no inciso anterior; ou

9.4.3.4 Impedimento de licitar e contratar com o Estado e descredenciamento no Cadastro Central de Fornecedores do Estado de Mato Grosso do Sul - CCF/MS pelo prazo de até cinco anos.

9.4.4 No caso de inexecução total ou parcial do objeto, a contratada estará sujeita à aplicação de multa de até 10% (dez por centro) do valor do contrato.

9.4.5 No caso de descumprimento do prazo estabelecido para a entrega do objeto do contrato, sem que haja justificativa aceita pela Contratante, a Contratada ficará sujeita à multa de 1% (um por cento) do valor empenhado, por dia de atraso, limitado à 10% (dez por cento). Após trinta dias de atraso, a Contratante poderá reconhecer a inexecução parcial ou total do contrato;

9.4.6 Em caso de subcontratação não autorizada, será aplicada multa de até 10% (dez por cento) do valor do contrato. A reincidência por uma vez de subcontratação não autorizada configurará inexecução parcial do contrato e ensejará a aplicação de

multa de 20% (vinte por cento) do valor do contrato, sem prejuízo da rescisão unilateral da avença;

9.4.7 Por infração a qualquer outra cláusula do Edital e seus Anexos, não prevista nos subitens anteriores, poderão ser aplicadas, isolada ou cumulativamente com outras sanções, inclusive a rescisão contratual, se for o caso:

9.4.7.1 Advertência, no caso de infrações leves;

9.4.7.2 Multa de até 10% (dez por cento):

9.4.7.2.1 Sobre o valor do item do qual participou a licitante, se a infração ocorrer durante a licitação; e

9.4.7.2.2 Sobre o valor do contrato, se a infração for ao contrato.

9.4.8 As penalidades serão aplicadas após regular processo administrativo, em que seja assegurado à licitante o contraditório e a ampla defesa, com os meios e recursos que lhes são inerentes;

9.4.9 Quaisquer multas aplicadas deverão ser recolhidas junto ao órgão competente no prazo de até 10 (dez) dias úteis contados de sua publicação no Diário Oficial do Estado de Mato Grosso do Sul, podendo, ainda, ser descontadas de qualquer fatura ou crédito existente, a critério da licitante;

9.4.10 Esgotados os meios administrativos para cobrança do seu valor à licitante, a multa será inscrita em dívida ativa;

9.4.11 A aplicação das sanções previstas nos itens 9.4.1 a 9.4.10 não excluem a possibilidade de aplicação de outras constantes da legislação que rege o tema, especialmente dos Decretos Estaduais n. 15.327, de 10 de dezembro 2019;

9.4.12 As sanções serão registradas no Cadastro Central de Fornecedores do Estado de Mato Grosso do Sul - CCF/MS.

10. ESTIMATIVA DE PREÇO E PREÇOS REFERENCIAIS

10.1 A estimativa de preço e preços referenciais integrará Anexo do respectivo instrumento convocatório.

11. ADEQUAÇÃO ORÇAMENTÁRIA

11.1 As despesas decorrentes do fornecimento correrão conforme segue:

Dotação			
Funcional Programática	Natureza de Despesa	Fonte de Recurso	Exercício.
110101 11101 04122000840010001	33904057	0100000000	2020

12. REGIME DE EXECUÇÃO DO CONTRATO (art. 9°, item X)

12.1 A Contratação será realizada através de Execução Indireta, em regime de empreitada por preço global.

13. CRITÉRIO DE JULGAMENTO DAS PROPOSTAS

13.1 O tipo de julgamento das propostas aplicado à contratação em tela é o de MENOR PREÇO POR ITEM;

13.2 A empresa participante deverá adicionar à proposta de preço para a participação deste certame, todos os catálogos técnicos, manuais e demais documentos necessários para a comprovação técnica das soluções ofertadas para cada item descrito neste Termo de Referência, sob pena de desclassificação.

14. PARCELAMENTO DO OBJETO

14.1 É sabido que o parcelamento da solução é a regra, devendo a licitação ser realizada por item sempre que o objeto for divisível, desde que se verifique não haver prejuízo para o conjunto da solução ou perda de economia de escala, visando propiciar a ampla participação de licitantes, que embora não disponham de capacidade para execução da totalidade do objeto, possam fazê-lo com relação a itens ou unidades autônomas;

14.2 Contudo, a contratação dos serviços em apreço em item único sem parcelamento é a que melhor atende aos interesses do Estado, pelas razões seguintes:

14.2.1 O produto citado é indivisível, não havendo possibilidade de fragmentar a solução para fornecimento parcelado, visto que não há viabilidade técnica para fracionar parte específica da solução para subcontratação deste ou ainda fragmentar os quantitativos, visto que se trata de produto que possui características intrínsecas de interoperabilidade e interdependência de seus diversos módulos;

14.2.2 Não há viabilidade para formação de consórcios, visto que a estrutura da solução é única, com mesma arquitetura e plataforma tecnológica, não cabendo tal formação para fornecimento de objeto uno e indivisível.

15. PARTICIPAÇÃO DE MICROEMPRESA E EMPRESA DE PEQUENO PORTE

15.1 A Lei Complementar n. 123/2006 vem dar tratamento diferenciado e simplificado à participação de ME e EPP e deve ser obrigatoriamente aplicada nas contratações da Administração Pública:

15.1.1 Após a realização de pesquisa de preços, providenciada pelo setor específico da Superintendência de Gestão de Compras e Materiais, é conhecida a composição do valor de cada item. Assim, caso o valor do Mapa Comparativo de Preços seja de até R$ 80.000,00 será aplicada a exclusividade na participação de ME/EPP conforme inciso I, art. 48, da Lei Complementar 123/2006. Caso o valor do Mapa Comparativo de Preços obtido seja superior a R$ 80.000,00 será aplicada a cota (25%) destinada a participação de ME/EPP, nos termos do inciso III, art. 48, da Lei Complementar n. 123/2006.

15.2 Insta mencionar que no art. 49, inciso III da lei acima mencionada, ressalta a impossibilidade de aplicação da lei, quando o tratamento diferenciado e simplificado para as microempresas e empresas de pequeno porte não for vantajoso para a administração pública;

15.3 No processo em tela, não há a possibilidade de aplicação do benefício previsto no Art. 48, inciso III, pelo fato da complexidade dos objetos a serem contratados, pois não há possibilidade da divisão dos mesmos itens de serviços para empresas distintas, sobre o aspecto técnico e econômico, demonstrando assim não ser vantajoso para administração pública a reserva de cota, tendo assim prejuízo ao conjunto ou ao complexo do objeto a ser contratado;

15.4 Por esta razão optamos pela não aplicação das regras do Art. 48, inciso III da Lei Complementar n. 123 de 14 de dezembro de 2006.

16. CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

16.1 REQUISITOS DE HABILITAÇÃO JURÍDICA:

16.1.1 Deverá ser verificado previamente à fase de habilitação, a existência de sanção que impeça a participação no certame ou a futura contratação, mediante consulta aos cadastros impeditivos de licitar ou contratar, em nome da empresa e de seus sócios.

16.1.2 Para a habilitação exigir-se-á dos interessados, exclusivamente, a documentação prevista no art. 27 da Lei nº 8.666, de 1993.

16.2 DA COMPROVACAO DAS CARACTERÍSTICAS TÉCNICAS DAS SOLUÇÕES OFERTADAS

16.2.1 A empresa participante deverá adicionar às demais documentações licitatórias obrigatórias para a participação deste certame, todos os catálogos técnicos, manuais e demais documentos necessários para a comprovação técnica das soluções ofertadas para cada item descrito neste Termo de Referência, sob pena de desclassificação.

16.3 QUALIFICAÇÃO TÉCNICA

16.3.1 Atestado(s) de Capacidade Técnica da licitante, emitido(s) por entidade da Administração Federal, Estadual ou Municipal, direta ou indireta e/ou empresa privada que comprove, de maneira satisfatória, a aptidão no fornecimento da solução compatível com o objeto desta contratação, conforme segue:

16.3.1.1 Justifica-se a exigência de Atestado de Capacidade Técnica tendo em vista a necessidade de se garantir que a empresa proponente detenha expertise no fornecimento e instalação de solução compatível com o objeto da licitação e na execução dos serviços de suporte e manutenção, considerando o grau de relevância e criticidade da rede WAN a ser atendida pela solução para continuidade da prestação dos serviços públicos sustentados;

16.3.1.2 Considera-se compatível com o objeto desta contratação a apresentação de atestado que comprove o fornecimento de até 50% (cinquenta por cento) dos quantitativos previstos neste documento, ou seja, o fornecimento de solução de proteção e otimização de tráfego em redes WAN para, pelo menos, 36 (trinta e seis) pontos de presença (localidades);

16.3.1.3 Para comprovação das quantidades mínimas exigidas, será permitida a somatória atestados, que demonstrem que o serviço tenha sido executado de forma simultânea (mesmo período), comprovando assim a capacidade de logística e infraestrutura da proponente em atender projetos deste porte e capacidade;

16.3.1.4 O(s) Atestado(s) deverá(ão) detalhar o escopo dos serviços prestados, compatível em características, quantidades e prazos com o objeto da licitação (conforme Art. 30, inciso II, da Lei nº 8.666/93), telefone e nome de pessoa de contato e declaração do cumprimento de todas as exigências técnicas e contratuais em nível satisfatório, em papel timbrado do emitente.

16.3.2 Certidão de registro da empresa e de seu responsável técnico, pertencente ao quadro técnico da licitante, na data prevista para entrega da proposta, no Conselho Regional de Engenharia e Agronomia (CREA), indicando assim, profissional técnico, adequado e disponível para a realização do objeto da licitação, conforme Art. 30, incisos I e II e § 1º, inciso I, da Lei nº 8.666/93.

16.3.2.1 A exigência de registro no CREA se justifica considerando que a instalação de sistemas de telecomunicações (como o caso dos equipamentos aqui descritos, que atuam sobre circuitos de comunicação que formam a rede WAN da SEFAZ/MS), são competência dos profissionais de engenharia, conforme prevê o art. 9° da Resolução CONFEA n. 218 de 29 de junho de 1973;

16.3.2.2 O requisito é indispensável para fins de apresentação de proposta no certame licitatório, visto que a apresentação de proposta demanda análise dos requisitos de telecomunicações presentes nas especificações deste termo, atividade esta que necessita de registro na entidade competente, para fins de legalidade no exercício regular da profissão, e está em consonância com o art. 30, inciso I da Lei n. 8666 de 1993;

16.4 REQUISITOS DE QUALIFICAÇÃO ECONÔNICO-FINANCEIRA

16.4.1 ÍNDICE DE SOLVÊNCIA

16.4.1.1 Como critério de habilitação, quanto à qualificação econômico-financeira, adota-se o Índice de Solvência Geral que deve ser maior ou igual a 1,0.

16.4.1.2 A seleção de licitantes com capacidade econômico-financeira suficiente para assegurar a execução integral do Contrato tem por dispositivo legal o artigo 31, §§1º e 5º da Lei n. 8.666/93. Assim, necessário se faz que a Administração Pública se previna de empresas sem quaisquer responsabilidades ou respaldo financeiro para a execução contratual e que não guardem capacidade financeira para assegurar o cumprimento do objeto da licitação até sua conclusão.

16.4.1.3 Referida capacidade financeira não diz respeito apenas ao cumprimento contratual, mas também a suportar possíveis atrasos no pagamento.

16.4.1.4 A Lei n. 8.666/93 não menciona de forma detalhada sobre o assunto, não havendo como definir um critério rígido para avaliar a conveniência do índice

exigido. A Norma Geral de Licitações não traz, assim, a obrigatoriedade de observância específica dos índices contábeis a serem postos no edital. Porém, a prática administrativa adotou a praxe dos índices contidos em instruções normativas.

16.4.1.5 Por óbvio, a Administração não quer contratar uma empresa que não tenha idoneidade financeira ou condições de executar um Contrato.

16.4.1.6 Assim, a Administração deve usar critérios usuais. Esses critérios foram estabelecidos lá atrás através da Instrução Normativa MARE-GM n. 5, de 21/7/1995 e prevalece, até hoje, da mesma forma, dispostos na Instrução Normativa n. 3, de 26/4/2018. Da redação dessa norma, a comprovação da boa situação financeira de empresa será baseada na obtenção de índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC).

16.4.1.7 Na falta de normatização estadual do índice de solvência para os editais de licitação, usamos como parâmetro normativo o índice "Solvência Geral" previsto na Instrução Normativa n. 3, de 26 de abril de 2018, do Ministério do Planejamento, Desenvolvimento e Gestão (atualizada), de forma a comprovar a boa situação financeira da empresa.

16.4.1.8 Assim temos como Solvência Geral (SG):

$$SG = \frac{\text{Ativo Total}}{\text{Passivo Circulante + Passivo Não-Circulante}} \geq 1$$

16.4.1.9 O índice de Solvência Geral expressa o grau de garantia que a empresa dispõe em Ativos (totais) para pagamento do total de suas dívidas. Envolve além dos recursos líquidos também os permanentes. O resultado ≥ 1 é recomendável à comprovação da boa situação financeira.

16.4.1.10 Ainda, caso as empresas não atingirem o índice acima previsto, poderá comprovar capital mínimo ou patrimônio líquido de 10% (dez por cento) do valor estimado da contratação.

16.4.1.11 Tal possibilidade está adequada, tendo em vista que, sobre o tema, a Súmula 275 do TCU assim dispõe: "Para fins de qualificação econômico-financeiro, a Administração pode exigir das licitantes, de forma não cumulativa, capital social mínimo, patrimônio líquido mínimo ou garantias que assegurem o

adimplemento do Contrato a ser celebrado, no caso de compras para entrega futura e de execução de obras e serviços. ”

16.4.1.12 Assim, optamos pela indicação de capital mínimo ou valor do patrimônio líquido de 10% (dez por cento), em virtude da exigência em porcentagem em grau máximo proteger as contratações efetuadas por este Estado.

16.5 Vistoria Técnica:

16.5.1 As proponentes poderão efetuar vistoria prévia nas dependências da Superintendência de Gestão da Informação/SGI, situada na Rua Delegado Osmar de Camargo, s/n, Parque dos Poderes, em Campo Grande/MS, para tomar ciência de todas as condições para a instalação dos equipamentos e prestação dos serviços.

16.5.1.1 A justificativa da vistoria prévia é fornecer aos licitantes, antes da elaboração de sua proposta de preços, o conhecimento real das condições do local onde serão executados os serviços, bem como esclarecimento de dúvidas quanto ao ambiente tecnológico para instalação dos equipamentos e softwares.

16.5.1.2 A visita poderá ser realizada em até 03 (três) dias úteis anterior ao dia da abertura do certame;

16.5.1.3 A visita deverá ser agendada junto a Superintendência de Gestão da Informação/SGI, pelo telefone (67) 3318-3517, no horário das 07h30min às 13h00hrs, de segunda a sexta-feira.

16.5.1.4 Será entregue Atestado de Vistoria Técnica lavrado e assinado pela Superintendência de Gestão da Informação/SGI, no ato da Visita Técnica.

16.5.1.5 O atestado de visita técnica deverá ser apresentado no certame pela licitante no envelope de proposta de preços.

16.5.1.6 A visita técnica terá espaço para dúvidas do licitante quanto ao conteúdo do Termo de Referência. Estará à disposição do licitante um técnico da SGI/SEFAZ/MS para esclarecimento das eventuais dúvidas.

16.5.1.7 Em nenhuma hipótese, o desconhecimento dos locais e de suas condições operacionais servirá como justificativa para a inexecução ou execução irregular do serviço a ser licitado.

17. ÍNDICE DE CORREÇÃO MONETÁRIA

17.1 Os preços serão fixos e irreajustáveis no prazo de um ano contado da data limite para a apresentação das propostas, após o que poderão sofrer reajuste aplicando-se o índice IGPM exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

17.2 O valor constante da nota fiscal/fatura, quando da sua apresentação, não sofrerá qualquer atualização monetária até o efetivo pagamento.

17.3 Caso o índice estabelecido para reajustamento venha a ser extinto ou de qualquer forma não possa mais ser utilizado, será adotado, em substituição, o que vier a ser determinado pela legislação então em vigor.

17.4 Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

17.5 O reajuste será realizado por apostilamento.

18. CLASSIFICAÇÃO DOS BENS COMUNS

18.1 Os objetos dessa licitação são classificados como bens comuns, pois possuem especificações usuais de mercado e padrões de qualidade definidas em Edital, nos termos do parágrafo único do art. 1º da Lei n. 10.520/02 e do inciso II e § 1º do art. 3º do Decreto estadual n. 15.327/19.

19. SUSTENTABILIDADE

19.1 De acordo com o art.3º da Lei n. 8.666/1993, a licitação destina-se a garantir, além de outros princípios, a promoção do desenvolvimento sustentável, harmonizando-se com o objetivo de selecionar a proposta mais vantajosa para a Administração;

19.2 A CONTRATADA adotará as seguintes práticas de sustentabilidade na execução dos serviços, quando couber:

19.2.1 Usar produtos de limpeza e conservação de superfícies e objetos inanimados que obedeçam às classificações e especificações determinadas pela ANVISA;

19.2.2 Realizar programa interno de treinamento de seus empregados, nos três primeiros meses de execução contratual, para redução de consumo de energia elétrica, de consumo de água e redução de produção de resíduos sólidos, observadas as normas ambientais vigentes;

19.2.3 Respeitar as Normas Brasileiras – NBR publicadas pela Associação Brasileira de Normas Técnicas sobre resíduos sólidos;

19.2.4 Que os bens sejam constituídos, no todo ou em parte, por material reciclado, atóxico, biodegradável, conforme ABNT NBR – 15448-1 e 15448-2. 15.8. Que os bens devam ser, preferencialmente, acondicionados em embalagem individual adequada, com o menor volume possível, que utilize materiais recicláveis, de forma a garantir a máxima proteção durante o transporte e o armazenamento;

19.2.5 Que os bens não contenham substâncias perigosas em concentração acima da recomendada na diretiva RoHS (Restriction of Certain Hazardous Substances), tais como mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr(VI)), cádmio (Cd), bifenilpolibromados (PBBs), éteres difenil-polibromados (PBDEs).

20. FRAUDE E CORRUPÇÃO

20.1 As licitantes e a contratada devem observar e fazer observar, por seus fornecedores e subcontratados, se admitida subcontratação, o mais alto padrão de ética durante todo o processo de licitação, de contratação e de execução do objeto contratual.

20.2 Para os propósitos do subitem 20.1, definem-se as seguintes práticas:

20.2.1 "**prática corrupta**": oferecer, dar, receber ou solicitar, direta ou indiretamente, qualquer vantagem com o objetivo de influenciar a ação de servidor público no processo de licitação ou na execução de contrato;

20.2.2 "**prática fraudulenta**": a falsificação ou omissão dos fatos, com o objetivo de influenciar o processo de licitação ou de execução de contrato;

20.2.3 "**prática conluiada**": esquematizar ou estabelecer um acordo entre dois ou mais licitantes, com ou sem o conhecimento de representantes ou prepostos do órgão licitador, visando estabelecer preços em níveis artificiais e não-competitivos;

20.2.4 "**prática coercitiva**": causar dano ou ameaçar causar dano, direta ou indiretamente, às pessoas ou sua propriedade, visando influenciar sua participação em um processo licitatório ou afetar a execução do contrato; e

20.2.5 "**prática obstrutiva**": (i) destruir, falsificar, alterar ou ocultar provas em inspeções ou fazer declarações falsas aos representantes do organismo financeiro multilateral, com o objetivo de impedir materialmente a apuração de alegações de prática prevista acima; e (ii) atos cuja intenção seja impedir materialmente o exercício do direito de o organismo financeiro multilateral promover inspeção.

20.3 Na hipótese de financiamento, parcial ou integral, por organismo financeiro multilateral, mediante adiantamento ou reembolso, este organismo imporá sanção sobre uma empresa ou pessoa física, inclusive declarando-a inidônea, indefinidamente ou por prazo determinado, para a outorga de contratos financiados pelo organismo se, em qualquer momento, constatar o envolvimento da empresa, diretamente ou por meio de um agente, em práticas corruptas, fraudulentas, colusivas, coercitivas ou obstrutivas ao participar da licitação ou da execução de um contrato financiado pelo organismo.

20.4 Considerando os propósitos dos subitens acima, a Contratada concorda e autoriza que, na hipótese de o contrato vir a ser financiado, em parte ou integralmente, por organismo financeiro multilateral, mediante adiantamento ou reembolso, o organismo financeiro e/ou pessoas por ele formalmente indicadas possam inspecionar o local de execução do contrato e todos os documentos, contas e registros relacionados à licitação e à execução do contrato.

21. ASSINATURA

Campo Grande, 02 de dezembro de 2020.

_____	_____
ALESSANDRO MENEZES DE SOUZA SUPERINTENDENTE SGI/SEFAZ/MS	GUSTAVO NANTES GUALBERTO ASSESSOR TÉCNICO SGI/SEFAZ/MS

Aprovado em: _____ / _____ / _____

_____

FELIPE MATTOS DE LIMA RIBEIRO
SECRETÁRIO DE ESTADO DE FAZENDA
SEFAZ/MS

ANEXO I "A"
MODELO DE PROPOSTA DE PREÇOS

Item	Especificação	Marca/ Modelo	Unid.	Qtd.	Vl. Unit.	Vl. Total.
001	Contratação de empresa especializada para fornecimento de solução envolvendo hardware, software, assinaturas de atualização, instalação, treinamento, customização e suporte em proteção e otimização de tráfego em redes WAN e proteção multicamadas contra ameaças avançadas em mensagens		Mês	12		

ANEXO I "B"
PLANILHA DE COMPOSIÇÃO DE CUSTOS E FORMAÇÃO DE PREÇOS

	Valor (R$)	Percentual (%)
Equipamentos		
Licenciamentos		
Depreciação dos equipamentos		
Serviços de instalação e configuração		
Serviço de suporte técnico e manutenção, incluindo NOC		
Despesas operacionais (diárias, deslocamento e outros)		
Despesas administrativas e indiretas		
Tributos e encargos		
Lucro		
TOTAL		100%