# ESTUDO TÉCNICO PRELIMINAR (BASEADO NO DECRETO n. 15.477/2020 E SEUS ANEXOS)

## 1. NECESSIDADE DA CONTRATAÇÃO (Decreto n. 15.477/2020, Art. 8°, I)

**1.1.** IDENTIFICAÇÃO DA NECESSIDADE DA CONTRATAÇÃO (Decreto n. 15.477/2020, Anexo I, Item 1):

1.1.1. A Equipe de Planejamento da Contratação elaborou o Estudo Técnico Preliminar com o objetivo de pesquisar uma Solução de Tecnologia da Informação e Comunicação (TIC) que proporcione **aceleração, segurança e otimização de tráfego de dados em rede WAN (Wide Área Network) e proteção multicamadas contra ameaças avançadas em mensagens eletrônicas para a infraestrutura de rede da SEFAZ/MS, em todos seus pontos de presença física**, para análise da sua viabilidade e levantamento dos elementos essenciais que servirão para compor o Termo de Referência, de forma que melhor atenda às necessidades da **SGI/SEFAZ-MS**, em conformidade com o disposto no art. 8° do Decreto Estadual n. 15.477 de 20 de julho de 2020.

1.1.2. A contratação será via Licitação na modalidade Pregão Eletrônico, conforme a Lei Federal nº 8.666/93, Lei Federal nº 10.520/2002 e Decreto Estadual 15.327/2019;

**1.2.** JUSTIFICATIVA DA NECESSIDADE DE CONTRATAÇÃO (Decreto n. 15.477/2020, Anexo I, Item 1.1):

1.2.1. 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.

1.2.2. 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.

1.2.3. 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.

1.2.4. 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.

1.2.5. 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.

1.2.6. 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.

1.2.7. 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.

1.2.8. 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.

1.2.9. 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.

1.2.10. 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.

1.2.11. 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.

**1.3.** CLASSIFICAÇÃO DO OBJETO DA CONTRATAÇÃO COMO SOLUÇÃO DE TIC (Decreto n. 15.477/2020, Art. 5°, Parágrafo Único):

1.3.1. O Decreto Estadual n. 15.477 de 20 de julho de 2020, em seu Art. 2°, XI, assim considera: “XI Solução de Tecnologia da Informação e Comunicação (STIC): conjunto de bens e/ou de serviços que apoiam processos de negócio, mediante a conjugação de recursos, processo e técnicas utilizados para obter, processar, armazenar, disseminar e fazer uso de informações”.

1.3.2. Em virtude disto, *o entendimento acerca da conceituação apresentada se baseia na* utilização *de bens* (hardware), sistemas de informação (software) e/ou *serviços de TIC, tendo como finalidade* o processamento de dados e informações digitais para *o alcance dos resultado*s pretendidos pela contratação.

1.3.3. Considerando que a solução em estudo engloba elementos com as características descritas acima, de modo a atender à necessidade que a desencadeou, pode-se afirmar que esta contratação compreende uma solução de tecnologia, e assim sendo deverá seguir as diretrizes estabelecidas no Decreto Estadual supracitado.

## 2. REQUISITOS DA CONTRATAÇÃO (Decreto n. 15.477/2020, Art. 8°, II)

**2.1.** REQUISITOS DE NEGÓCIO (Decreto n. 15.477/2020, Anexo I, Item 2.2.1):

2.1.1. O presente estudo técnico 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:

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

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

2.1.1.3. Alta disponibilidade de rede, em modo Ativo/Standby;

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

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

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

2.1.1.7. Filtragem de URL para gerenciamento e controle de acessos.

2.1.1.8. Proteção antivírus e anti-bot;

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

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

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

2.1.2.1. Serviço de garantia de hardware para toda a infraestrutura fornecida;

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

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

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

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

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

**2.2.** REQUISITOS LEGAIS (Decreto n. 15.477/2020, Anexo I, Item 2.2.2):

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

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

2.2.3. 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.

**2.3.** REQUISITOS DE ARQUITETURA TECNOLÓGICA (Decreto n. 15.477/2020, Anexo I, Item 2.2.3):

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

2.3.1.1. Requisitos de Capacidade e de Interfaces:

2.3.1.1.1. 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;

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

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

2.3.1.1.4. Performance de IPS de 5 Gbps ou superior;

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

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

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

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

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

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

2.3.1.1.11. Deverá possuir pelo menos oito interfaces de 1 GbE SFP;

2.3.1.1.12. 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:

2.3.1.1.12.1. Segmento WAN, ou externo;

2.3.1.1.12.2. 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;

2.3.1.1.12.3. Segmento LAN ou rede interna;

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

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

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

2.3.1.1.13. 01 (uma) interface de rede dedicada para gerenciamento;

2.3.1.1.14. 01 (uma) interface do tipo console ou similar;

2.3.1.1.15. 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;

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

2.3.1.1.17. Suportar, no mínimo, 5 Gbps de throughput de VPN IPSEC;

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

2.3.1.2. Requisitos Gerais:

2.3.1.2.1. 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;

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

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

2.3.1.2.4. 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;

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

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

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

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

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

2.3.1.2.10. 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;

2.3.1.2.11. 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;

2.3.1.2.12. 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;

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

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

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

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

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

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

2.3.1.2.15.4. 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;

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

2.3.1.2.16. Possuir DHCP Server interno;

2.3.1.2.17. 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;

2.3.1.2.18. Suporte a Jumbo Frames;

2.3.1.2.19. Implementar sub-interfaces ethernet lógicas;

2.3.1.2.20. 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;

2.3.1.2.21. Suportar NAT de origem e NAT de destino simultaneamente;

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

2.3.1.2.23. 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;

2.3.1.2.24. 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;

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

2.3.1.2.26. Permitir remarcação de pacotes utilizando TOS e/ou DSCP;

2.3.1.2.27. 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;

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

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

2.3.1.2.30. Suportar Equal Cost Multi-Path (ECMP);

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

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

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

2.3.1.2.34. 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;

2.3.1.2.35. Possui suporte a log via syslog;

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

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

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

2.3.1.2.39. 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.

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

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

2.3.1.3. Requisitos de Alta Disponibilidade:

2.3.1.3.1. 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;

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

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

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

2.3.1.4. Requisitos de VPN (Virtual Private Network):

2.3.1.4.1. 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;

2.3.1.4.2. Criptografia 3DES, AES 128 e AES 256;

2.3.1.4.3. Autenticação com MD5, SHA-1, SHA-256 e SHA-384;

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

2.3.1.4.5. Algoritmo Internet Key Exchange (IKE);

2.3.1.4.6. Autenticação via certificado IKE PKI;

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

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

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

2.3.1.4.10. 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;

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

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

2.3.1.4.13. 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;

2.3.1.4.14. 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.

2.3.1.5. Requisitos de Autenticação:

2.3.1.5.1. 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;

2.3.1.5.2. Permitir a utilização de LDAP, AD e RADIUS;

2.3.1.5.3. 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;

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

2.3.1.5.5. 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;

2.3.1.5.6. 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;

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

2.3.1.5.8. 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.

2.3.1.6. Requisitos de IPS (Intrusion Prevention System):

2.3.1.6.1. 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;

2.3.1.6.2. 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;

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

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

2.3.1.6.5. 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;

2.3.1.6.6. Possuir capacidade de remontagem de pacotes para identificação de ataques;

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

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

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

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

2.3.1.6.11. A solução deve ser capaz de inspecionar tráfego HTTPS;

2.3.1.6.12. 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;

2.3.1.6.13. Deverá possuir capacidade de detecção de anomalias;

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

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

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

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

2.3.1.6.18. 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;

2.3.1.6.19. Deve incluir proteção contra worms;

2.3.1.6.20. 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;

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

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

2.3.1.6.23. 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);

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

2.3.1.6.25. A solução deverá possuir proteções para sistemas SCADA;

2.3.1.6.26. 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;

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

2.3.1.7. Requisitos de Controle de Aplicação:

2.3.1.7.1. 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);

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

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

2.3.1.7.4. 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;

2.3.1.7.5. 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;

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

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

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

2.3.1.7.9. Atualizar a base de assinaturas de aplicações automaticamente;

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

2.3.1.7.11. 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;

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

2.3.1.7.13. 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;

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

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

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

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

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

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

2.3.1.7.19.1. Nível de risco da aplicação.

2.3.1.7.19.2. Categoria de aplicações.

2.3.1.8. Requisitos de Filtragem de URL (Uniform Resource Locator):

2.3.1.8.1. 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;

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

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

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

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

2.3.1.8.6. 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).

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

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

2.3.1.8.9. Deverá permitir criar política de confirmação de acesso;

2.3.1.8.10. 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;

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

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

2.3.1.8.13. 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);

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

2.3.1.8.15. 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;

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

2.3.1.8.17. 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;

2.3.1.8.18. Possuir pelo menos 50 categorias de URLs;

2.3.1.8.19. Suporta a criação de categorias de URLs customizadas;

2.3.1.8.20. Suporta a exclusão de URLs do bloqueio, por categoria;

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

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

2.3.1.8.23. Permitir a customização de página de bloqueio.

2.3.1.9. Requisitos de Proteção Contra Vírus e Botnets:

2.3.1.9.1. 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;

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

2.3.1.9.3. 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;

2.3.1.9.4. 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;

2.3.1.9.5. Implementar funcionalidade de detecção e bloqueio de callbacks;

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

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

2.3.1.9.8. Implementar interface gráfica WEB segura, utilizando o protocolo HTTPS;

2.3.1.9.9. Implementar interface CLI segura através do protocolo SSH;

2.3.1.9.10. 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;

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

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

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

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

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

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

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

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

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

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

2.3.1.9.21. 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.

2.3.1.10. Requisitos de Proteção para Ataques Avançados:

2.3.1.10.1. 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;

2.3.1.10.2. 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;

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

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

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

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

2.3.1.10.7. 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;

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

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

2.3.1.10.10. 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;

2.3.1.10.11. 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.

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

2.3.1.10.13. 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;

2.3.1.10.14. Conter ameaças avançadas de dia zero;

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

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

2.3.1.10.17. 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;

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

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

2.3.1.10.20. 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;

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

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

2.3.1.10.23. Implementar mecanismo de pesquisa por diferentes intervalos de tempo;

2.3.1.10.24. Conter ameaças de dia zero via tráfego de internet;

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

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

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

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

2.3.1.10.29. Conter exploits avançados;

2.3.1.10.30. 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);

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

2.3.1.11. Requisitos de Administração:

2.3.1.11.1. 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;

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

2.3.1.11.3. Políticas baseadas por grupos de usuários deverão ser suportadas;

2.3.1.11.4. 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;

2.3.1.11.5. Fornecer gerência remota, com interface gráfica nativa;

2.3.1.11.6. 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;

2.3.1.11.7. 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;

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

2.3.1.11.9. 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;

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

2.3.1.11.11. 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;

2.3.1.11.12. 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;

2.3.1.11.13. 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;

2.3.1.11.14. 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;

2.3.1.11.15. 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;

2.3.1.11.16. 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;

2.3.1.11.17. 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.

2.3.1.12. Requisitos de Proteção Multicamadas Contra Ameaças Avançadas em Mensagens:

2.3.1.12.1. 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;

2.3.1.12.2. 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;

2.3.1.12.3. 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;

2.3.1.12.4. Especificações de Software:

2.3.1.12.4.1. Ser um MTA completo com suporte ao protocolo SMTP;

2.3.1.12.4.2. Possuir filtros de reputação;

2.3.1.12.4.3. Possuir solução antispam integrada;

2.3.1.12.4.4. Possuir solução antiphishing integrada;

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

2.3.1.12.4.6. Possuir módulo de consulta customizada e impressão de relatórios estatísticos;

2.3.1.12.4.7. Possuir a funcionalidade de SPF;

2.3.1.12.4.8. Possuir a funcionalidade de DKIM;

2.3.1.12.4.9. Possuir a funcionalidade de DMARC.

2.3.1.12.5. Interface de Administrador:

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

2.3.1.12.5.2. A interface gráfica deverá permitir acesso via HTTPS;

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

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

2.3.1.12.5.5. 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.

2.3.1.12.6. Especificações do MTA:

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

2.3.1.12.6.2. 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;

2.3.1.12.6.2.1. Deverão suportar RBL (listagem baseada em DNS);

2.3.1.12.6.2.2. Deverão possuir e utilizar filtros de reputação;

2.3.1.12.6.2.3. 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.

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

2.3.1.12.6.4. Deverá ser capaz de utilizar DNS reverso nas conexões de entrada;

2.3.1.12.6.5. Deverá ser capaz de processar o seguinte tráfego de mensagens:

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

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

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

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

2.3.1.12.6.8. 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;

2.3.1.12.6.9. 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;

2.3.1.12.6.10. Deverá suportar "aliasing";

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

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

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

2.3.1.12.6.14. 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;

2.3.1.12.6.15. 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;

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

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

2.3.1.12.7. Especificações dos filtros de reputação:

2.3.1.12.7.1. 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;

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

2.3.1.12.7.3. 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;

2.3.1.12.7.4. 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.

2.3.1.12.8. Especificações do software antispam:

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

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

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

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

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

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

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

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

2.3.1.12.8.9. Permitir a proteção contra phishings;

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

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

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

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

2.3.1.12.8.14. 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;

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

2.3.1.12.8.16. 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);

2.3.1.12.8.17. 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;

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

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

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

2.3.1.12.9. Especificações de Segurança do MTA:

2.3.1.12.9.1. 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;

2.3.1.12.9.2. 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;

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

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

2.3.1.12.9.5. 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;

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

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

2.3.1.12.10. Especificações de Filtros de Segurança:

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

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

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

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

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

2.3.1.12.10.6. Permitir o escaneamento de arquivos executáveis comprimidos em tempo real;

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

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

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

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

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

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

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

2.3.1.12.11. Especificações de Atualização e Administração do MTA:

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

2.3.1.12.11.2. 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;

2.3.1.12.11.3. Possibilidade de agendamento e envio dos relatórios por e-mail;

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

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

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

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

2.3.1.12.11.8. 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);

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

2.3.1.12.11.10. 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);

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

2.3.1.12.11.12. 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”;

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

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

2.3.1.12.11.15. 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;

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

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

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

2.3.1.12.11.19. Possuir autenticação via TLS (Transport Layer Security);

2.3.1.12.11.20. Ter gerencia de área exclusiva para quarentena ou cópia de mensagens;

2.3.1.12.11.21. 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”;

2.3.1.12.11.22. 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);

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

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

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

2.3.1.12.11.26. Permitir exclusão automática das mensagens em quarentena;

2.3.1.12.11.27. 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;

2.3.1.12.11.28. 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;

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

2.3.1.12.11.30. Possuir funcionalidade de criação de “alias” e mascaramento de endereço;

2.3.1.12.11.31. 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.

2.3.2. Requisitos Específicos para os Appliances dos SITES REMOTOS:

2.3.2.1. 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;

2.3.2.2. 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;

2.3.2.3. 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;

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

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

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

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

2.3.2.8. A solução oferecida deve prover administração através de interface WEB;

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

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

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

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

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

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

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

2.3.2.16. A solução deverá oferecer o serviço de filtro de conteúdo;

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

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

2.3.3.1. 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;

2.3.3.2. 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;

2.3.3.3. 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;

2.3.3.4. 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;

2.3.3.5. Em se tratando de "appliance virtual", a Contratada deverá fornecer plataforma de hardware compatível para a instalação da solução;

2.3.3.6. 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;

2.3.3.7. 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;

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

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

2.3.3.10. 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:

2.3.3.10.1. Utilização do algoritmo HFSC (Hierarquical Fair Service Curves);

2.3.3.10.2. Suporte a variados tipos/filas de priorização de serviços simultaneamente;

2.3.3.10.3. Limitação de quantidade de conexões simultâneas;

2.3.3.10.4. Classificação das aplicações por endereços IP e Portas;

2.3.3.10.5. Especificação de VLAN para as regras;

2.3.3.10.6. Garantia de um mínimo de banda para uma determinada aplicação;

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

2.3.3.11. 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;

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

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

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

2.3.3.15. A solução deve prover aceleração de compartilhamento de arquivos Windows;

2.3.3.16. A solução deve prover aceleração de CIFS;

2.3.3.17. A solução deve prover aceleração de SMB assinado;

2.3.3.18. A solução deve prover otimização de protocolo;

2.3.3.19. A solução deve prover visualização de WFS;

2.3.3.20. A solução deve prover visualização de TCP;

2.3.3.21. A solução deve prover compressão de dados;

2.3.3.22. A solução deve prover diminuição de latência de rede;

2.3.3.23. A solução deve suportar SNMP e Syslog;

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

2.3.3.25. 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;

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

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

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

2.3.4. Requisitos do Software de Gerenciamento

2.3.4.1. 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;

2.3.4.2. 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:

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

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

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

2.3.4.2.4. A solução deverá prover painel de visualização geral das soluções;

2.3.4.2.5. A solução deverá prover visualização de logs em tempo real;

2.3.4.2.6. 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;

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

2.3.4.2.8. 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);

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

2.3.4.2.10. 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;

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

2.3.4.2.12. 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).

**2.4.** REQUISITOS DE PROJETO E DE IMPLEMENTAÇÃO (Decreto n. 15.477/2020, Anexo I, Item 2.2.4):

2.4.1. Não se aplica.

**2.5.** REQUISITOS DE IMPLANTAÇÃO (Decreto n. 15.477/2020, Anexo I, Item 2.2.5):

2.5.1. Diagrama Proposto:

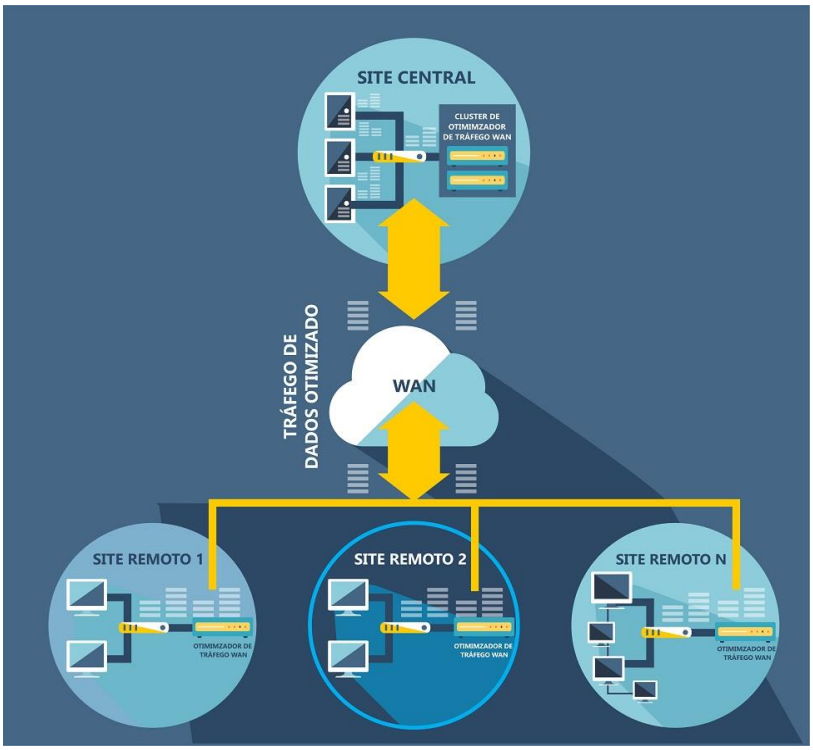


**Figura 1 - Diagrama da Solução de Otimização de Tráfego WAN**

2.5.2. Localidades Atendidas:

2.5.2.1. SITE CENTRAL

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

2.5.2.2. 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<br>Setor de Fiscalização Regional Norte<br>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<br>Subunidade de Fiscalização de Mercadorias em Transportadoras de Dourados<br>Subunidade de Fiscalização Externa Sul | Rua Joaquim Teixeira Alves n. 1616 - Centro<br>Rua Antonio Emilio de Figueiredo n. 1860 - Centro<br>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<br>Agência Fazendária de Três Lagoas Setor Transportadora de Três Lagoas | Av. Capitão Olinto Mancini n. 2462 | Três Lagoas |

2.5.3. Entrega e Instalação:

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

2.5.3.2. 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;

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

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

2.5.3.5. 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;

2.5.3.6. 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;

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

2.5.3.8. 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;

2.5.3.9. 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;

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

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

**2.6.** REQUISITOS TEMPORAIS (Decreto n. 15.477/2020, Anexo I, Item 2.2.6):

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

2.6.2. 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;

2.6.3. 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:

2.6.3.1. Identificação de cada chamado;

2.6.3.2. Identificação do tipo de atendimento;

2.6.3.3. Data de atendimento (abertura e conclusão);

2.6.3.4. Descrição do atendimento;

2.6.3.5. Procedimentos adotados para a solução do problema;

2.6.3.6. 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.

**2.7.** REQUISITOS DE GARANTIA E MANUTENÇÃO (Decreto n. 15.477/2020, Anexo I, Item 2.2.7):

2.7.1. 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;

2.7.2. 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:

2.7.2.1. 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;

2.7.2.2. 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;

2.7.2.3. 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;

2.7.2.4. 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.

2.7.3. Tipos de serviços de suporte técnico e manutenção:

2.7.3.1. 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:

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

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

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

2.7.3.1.4. 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;

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

2.7.3.2. 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:

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

2.7.3.2.2. 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;

2.7.3.2.3. Corrigir defeitos de fabricação ou projeto;

2.7.3.2.4. 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;

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

2.7.3.2.6. 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;

2.7.3.2.7. 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.

2.7.4. Suporte técnico especializado e manutenção prestados pela Contratada:

2.7.4.1. 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;

2.7.4.2. 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;

2.7.4.3. 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;

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

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

2.7.4.6. 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;

2.7.4.7. 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;

2.7.4.8. 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;

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

2.7.4.10. 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;

2.7.4.11. 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;

2.7.4.12. 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:

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

2.7.4.12.2. 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;

2.7.4.12.3. 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.

2.7.4.13. 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;

2.7.4.14. 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.

2.7.5. Suporte técnico especializado e manutenção prestados pelo Fabricante:

2.7.5.1. 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:

2.7.5.1.1. 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);

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

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

2.7.6. 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:

2.7.6.1. 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;

2.7.6.2. 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.

2.7.7. Núcleo de Operações e Controle:

2.7.7.1. 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;

2.7.7.2. 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 soluções ofertadas, para prestar o pronto-atendimento as solicitações de suporte de primeiro e segundo nível identificadas no NOC e/ou usuários finais das soluções.

**2.8.** REQUISITOS DE CAPACITAÇÃO (Decreto n. 15.477/2020, Anexo I, Item 2.2.8):

2.8.1. 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;

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

2.8.3. 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;

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

2.8.5. 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;

2.8.6. 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;

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

2.8.7.1. Instalação do produto;

2.8.7.2. Utilização da interface gráfica simples;

2.8.7.3. Configuração dos parâmetros básicos e gerenciamento de usuários;

2.8.7.4. Melhores práticas de utilização da solução;

2.8.7.5. Integração com ambientes de virtualização;

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

2.8.7.7. Criação de perfis de aceleração e otimização de rede e aplicações;

2.8.7.8. Configuração de ambiente de alta disponibilidade (cluster);

2.8.7.9. Configuração de parâmetros para balanceamento de carga de serviços;

2.8.7.10. Conceitos de monitoramento;

2.8.7.11. Processamento de tráfego SSL na solução.

2.8.8. 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;

2.8.9. 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.

**2.9.** REQUISITOS DE EXPERIÊNCIA PROFISSIONAL DA EQUIPE (Decreto n. 15.477/2020, Anexo I, Item 2.2.9):

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

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

2.9.2.1. 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.* |

2.9.2.2. 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.* |

2.9.2.3. 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.*<br>*Certificado de conclusão ISO/IEC 20000, fornecido por instituto credenciado.* |
| ***Formação*** | ***Modo de Comprovação*** |
| *Não se aplica.* | *Não se aplica.* |

2.9.3. 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:

2.9.3.1. Carteira de Trabalho e Previdência Social (CTPS);

2.9.3.2. Contrato de Prestação de Serviços, no caso de profissional autônomo;

2.9.3.3. Contrato Social, no caso de sócio proprietário.

**2.10.** REQUISITOS DE FORMAÇÃO DA EQUIPE (Decreto n. 15.477/2020, Anexo I, Item 2.2.10):

2.10.1. Não se aplica.

**2.11.** REQUISITOS DE METODOLOGIA DE TRABALHO (Decreto n. 15.477/2020, Anexo I, Item 2.2.11):

2.11.1. Não se aplica.

**2.12.** REQUISITOS DE SEGURANÇA DA INFORMAÇÃO (Decreto n. 15.477/2020, Anexo I, Item 2.2.12):

2.12.1. 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.

2.12.2. 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.

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

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

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

2.12.6. 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.

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

**2.13.** REQUISITOS SOCIAIS, AMBIENTAIS E CULTURAIS (Decreto n. 15.477/2020, Anexo I, Item 2.2.13):

2.13.1. 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.

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

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

2.13.4. 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.

## 3. ESTIMATIVA DAS QUANTIDADES PARA CONTRATAÇÃO (Decreto n. 15.477/2020, Art. 8°, III)

**3.1.** As quantidades a serem contratadas foram definidas da seguinte forma:

3.1.1. Cada ponto de presença da SEFAZ/MS na capital e interior do Estado, constantes na tabela do item 2.5.2.1, é atendido por um circuito WAN interligando-o ao Site Central (SGI), estes fornecidos por operadora de Telecom contratada.

3.1.2. Cada ponto remoto necessita de uma solução de menor porte, atendendo aos requisitos necessários e já especificados.

3.1.3. Já o Site Central (SGI) que recebe a conexão com cada ponto remoto e consolida a rede WAN da SEFAZ/MS, necessita de uma solução mais robusta em termos de

capacidade e que tenha mais recursos, para prover as funcionalidades necessárias para proteção e otimização da rede.

3.1.4. Neste sentido, foram definidos os seguintes quantitativos:

3.1.4.1. 1 (uma) unidade de Appliance para o Site Central (SGI), conforme requisitos do item 2.3.1;

3.1.4.1.1. Para ampliar a quantidade de soluções possíveis, caso determinado fabricante não possua as funções descritas no item 2.3.1.12 (Proteção Multicamadas Contra Ameaças Avançadas em Mensagens) no mesmo Appliance citado acima, poderá fornecê-las em 1 (uma) unidade de Appliance adicional, podendo este ser físico (equipamento), Appliance virtual ou solução em nuvem fornecido pela Contratada;

3.1.4.2. 72 (setenta e duas) unidades de Appliance para os Sites Remotos, conforme requisitos do item 2.3.2, a serem instaladas em cada uma das localidades constantes na tabela do item 2.5.2.2;

3.1.4.2.1. Para ampliar a quantidade de soluções possíveis, caso determinado fabricante não possua as funções descritas no item 2.3.3 (Aceleração WAN) no mesmo Appliance fornecido para o Site Central (SGI) e Sites Remotos, poderá fornecer uma unidade adicional de Appliance para cada uma das localidades a serem atendidas, com todos os requisitos constantes no item 2.3.3.

3.1.4.3. 1 (uma) unidade do Software de Gerenciamento, conforme requisitos do item 2.3.4.

**3.2.** Não há memória de cálculo a ser anexada a este estudo, considerando que os quantitativos descritos e as localidades a serem atendidas já estão previstas no corpo deste documento, conforme item 2.5.2.

## 4. ANÁLISE COMPARATIVA DE SOLUÇÕES EXISTENTES (Decreto n. 15.477/2020, Art. 8°, IV)

**4.1.** Dentro do presente estudo, foram analisados processos de contratações semelhantes feitas por outros órgãos e entidades, por meio de consultas a outros editais, com a finalidade de identificar a existência de novas metodologias, tecnologias ou inovações que melhor atendessem às necessidades, e as que foram identificadas foram incorporadas nesta contratação em análise.

**4.2.** Foram analisadas as seguintes alternativas para atendimento às necessidades elencadas:

4.2.1. **Cenário (1)**: Outsourcing da Solução: incluindo o fornecimento de solução como serviço, envolvendo hardware, software, assinaturas de atualização, instalação, treinamento, customização, suporte técnico e manutenção.

4.2.2. **Cenário (2)**: Aquisição de hardware: inclui a aquisição de todos os equipamentos e dos softwares, sem a contratação dos serviços de assinaturas de atualização, instalação, treinamento, customização, suporte técnico e manutenção, estes ficando a cargo da Administração.

**4.3.** A análise comparativa das soluções observou as seguintes diretrizes (Decreto n. 15.477/2020, Anexo I, Item 3):

| Diretriz | Cenário (1) | Cenário (2) |
|---|---|---|
| Aderência aos padrões tecnológicos adotados pelo Estado *(Decreto n. 15.477/2020, Anexo I, Item 3.1)* | A solução atende aos padrões tecnológicos adotados pelo Estado. | A solução não atende aos padrões tecnológicos adotados pelo Estado. |
| Disponibilidade de solução de TIC similar em outro órgão ou entidade da Administração Pública *(Decreto n. 15.477/2020, Anexo I, Item 3.2)* | Encontramos a utilização deste modelo de solução de TIC em diversos outros editais e contratos da Administração Pública. | Não encontramos a utilização deste modelo de solução de TIC em outros editais e contratos da Administração Pública. |
| Alternativas do mercado, inclusive quanto a existência de software livre ou gratuito *(Decreto n. 15.477/2020, Anexo I, Item 3.3)* | Não foram encontradas soluções envolvendo software livre ou gratuito. | Não foram encontradas soluções envolvendo software livre ou gratuito. |
| Aderência às regulamentações da ICP-Brasil e modelo eARQ *(Decreto n. 15.477/2020, Anexo I, Item 3.4)* | Não se aplica | Não se aplica |
| Necessidades de adequação do ambiente *(Decreto n. 15.477/2020, Anexo I, Item 3.5)* | Não é necessário adequar o ambiente do órgão ou entidade para implantar a solução | Não é necessário adequar o ambiente do órgão ou entidade para implantar a solução |
| Diferentes modelos de prestação dos serviços *(Decreto n. 15.477/2020, Anexo I, Item 3.6)* | Este modelo preconiza a contratação de solução através dos conceitos atuais de IAAS (infraestrutura como serviço). Tem sido amplamente utilizada, é estabelece a terceirização integral dos serviços. | Este modelo é estabelece a aquisição de toda a plataforma, agregando os equipamentos e softwares ao patrimônio, e mantém o encargo de gestão e controle da solução para o Estado. |
| Diferentes tipos de soluções em termos de especificação, composição ou características *(Decreto n. 15.477/2020, Anexo I, Item 3.7)* | Independente da solução a ser adotada, todas deverão possuir especificação e características semelhantes. | Independente da solução a ser adotada, todas deverão possuir especificação e características semelhantes. |
| Possibilidade de aquisição na forma de bens ou contratação como serviço *(Decreto n. 15.477/2020, Anexo I, Item 3.8)* | A solução prevê a contratação integralmente como serviço. | A solução prevê a aquisição (fornecimento) de bens. |
| Ampliação ou substituição da solução implantada *(Decreto n. 15.477/2020, Anexo I, Item 3.9)* | Ampliação e substituição viável, através de nova contratação ou aditivo ao contrato de prestação de serviços | Ampliação viável, através de aquisição de novos bens. A substituição irá demandar nova aquisição e substituição de todo o patrimônio adquirido. |

## 5. ESCOLHA DA STIC E JUSTIFICATIVA DA OPÇÃO ADOTADA (Decreto n. 15.477/2020, Art. 8°, V)

**5.1.** Dentre as soluções passíveis de atendimento as necessidades levantadas, optamos pela constante no Cenário (1): Outsourcing da Solução, incluindo o fornecimento de solução

como serviço, envolvendo hardware, software, assinaturas de atualização, instalação, treinamento, customização, suporte técnico e manutenção, considerando as seguintes motivações:

**5.2.** JUSTIFICATIVA QUANTO À SOLUÇÃO ESCOLHIDA (Decreto n. 15.477/2020, Anexo I, Item 4.1):

5.2.1. A contratação através da aquisição não é tecnicamente vantajosa, visto que:

5.2.1.1. As tecnologias de informação, no caso as de proteção, segurança da informação e otimização de redes são diariamente atualizadas, com novas assinaturas de combate e prevenção de ameaças, disponibilização de novos recursos, atualização dos filtros de conteúdo, dentre outros aspectos. Adquirir os equipamentos não garante essa atualização constante, o que em curto período de tempo tornará o ativo adquirido obsoleto e inservível, obrigando o Estado a substituir constantemente a tecnologia já implantada, sob o risco de não garantir a proteção e continuidade de serviços necessária;

5.2.1.2. Esse fator justifica a ausência do cenário de aquisição em outros processos da Administração Pública, visto que não há viabilidade técnica de se manter a solução sem as atualizações fornecidas pela fabricante;

5.2.1.3. A SEFAZ/MS não dispõe de expertise técnica e nem faz parte de seu objetivo possuir analistas de segurança da informação que façam a pesquisa, investigação, desenvolvimento e homologação de soluções avançadas de segurança de rede, o que justifica buscar empresa especializada no mercado para esta finalidade;

5.2.1.4. O outsourcing da solução proporciona a gestão efetiva dos dados e informações que trafegam na rede e que, em consequência, possibilita a obtenção de indicadores de qualidade, desempenho, disponibilidade, utilização de recursos e custos de forma mais ágil e exata, permitindo melhor planejamento, tomadas de decisão e ações rápidas, cada vez mais demandadas pelas Unidades, especialmente as finalísticas;

5.2.1.5. Em consequência, o cenário adotado reduz de forma drástica as interrupções do serviço devido as manutenções corretivas, através da implantação e aplicação de acordos de níveis de serviço (Service Level Agreement - SLA).

**5.3.** DESCRIÇÃO DA SOLUÇÃO (Decreto n. 15.477/2020, Anexo I, Item 4.2):

5.3.1. 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.

**5.4.** ALINHAMENTO EM RELAÇÃO ÀS NECESSIDADES E REQUISITOS INDICADOS (Decreto n. 15.477/2020, Anexo I, Item 4.3):

5.4.1. A solução escolhida irá atender às necessidades apontadas neste estudo, pois o objeto a ser contratado abrange a contração de empresa especializada para a prestação de serviços com o fornecimento de toda a solução, deste a aquisição dos hardwares, software, assinaturas de atualização, passando pela instalação, treinamento e customização, além do serviço de suporte.

**5.5.** IDENTIFICAÇÃO DOS BENEFÍCIOS A SEREM ALCANÇADOS (Decreto n. 15.477/2020, Anexo I, Item 4.4):

5.5.1. Aceleração das aplicações e sistemas de informação utilizados nas Agências Fazendárias, Postos Fiscais e demais unidades Fazendárias, ampliando a produtividade e agilidade no atendimento ao contribuinte e na prestação dos serviços públicos;

5.5.2. Diminuição da latência de rede nos circuitos de comunicação de dados entre as unidades Fazendárias e a SGI, evitando a interrupção dos serviços e aumentando a continuidade das soluções de TI trafegadas em rede;

5.5.3. Maior disponibilidade de recursos para as ações efetivas do Executivo;

5.5.4. Maior controle e gerência da SGI/SEFAZ-MS quando ao acesso às redes locais e aos sistemas de informação utilizados, bem como garantia do combate proativo e reativo frente às ameaças eletrônicas e a perda de dados e informações críticas e/ou sigilosas;

5.5.5. Cumprir com o compromisso e premissas básicas do Governo do Estado de oferecer acesso com desempenho maior e disponibilidade de recursos.

**5.6.** DECLARAÇÃO (Decreto n. 15.477/2020, Anexo I, Item 4.5):

5.6.1. Declaramos que foram observadas as vedações constantes no art. 2º do Decreto Estadual n. 15.477 de 20 de julho de 2020, notadamente a impossibilidade de não ser objeto de contratação de Solução de TIC mais de uma solução em um único contrato, e gestão de processos de Tecnologia da Informação e Comunicação (incluindo gestão de segurança da informação).

**5.7.** METODOLOGIA DE AVALIAÇÃO DA QUALIDADE E DA ADEQUAÇÃO (Decreto n. 15.477/2020, Anexo I, Item 4.6):

5.7.1. A avaliação da qualidade e adequação da Solução de Tecnologia da Informação às especificações funcionais e tecnológicas será realizada através da verificação de atendimento aos requisitos e emissão dos Termos de Recebimento Provisório e Definitivo e Acordo de Níveis de Serviço.

**5.8.** DEFINIÇÃO DA FORMA DE REMUNERAÇÃO (Decreto n. 15.477/2020, Anexo I, Item 4.7):

5.8.1. A remuneração dos serviços previstos neste estudo será realizada através de pagamento de valor fixo mensal, conforme critérios a serem descritos no Termo de Referência.

## 6. JUSTIFICATIVA PARA O PARCELAMENTO OU NÃO DO OBJETO (Decreto n. 15.477/2020, Art. 8°, VI)

**6.1.** 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.

**6.2.** Contudo, a contratação dos serviços em apreço em item único sem parcelamento é a que melhor atende as necessidades da SEFAZ/MS, pelas razões seguintes:

6.2.1. A solução deve ser adquirida de maneira completa, pois perfazem uma única solução, uma vez que os equipamentos devem ser compatíveis entre si e com os softwares de gerenciamento. Ao fragmentar as aquisições, não será possível garantir a compatibilidade dos itens de hardware e dos softwares a serem instalados;

6.2.2. Por se tratar de uma solução integrada, constituída por funcionalidades e serviços intrinsecamente ligados entre si, e considerando que todos os componentes devem ser de um mesmo fabricante, bem, como o serviço de suporte que devem ser realizados por profissional especializado na solução, não há viabilidade técnica para o parcelamento da solução por itens;

6.2.3. Não avaliamos restrição de mercado ao adquirir a solução de maneira global, visto que individualmente tratam-se de bens e materiais de uso comum e de requisitos padronizados, não havendo dificuldade das empresas em providenciar os bens e prestar os serviços requisitados;

6.2.4. No caso em análise, os serviços citados são indivisíveis, não havendo possibilidade de contratar o suporte técnico e a manutenção de fornecedores diferentes, tendo em vista que são serviços caracterizados pela interoperabilidade e interdependência, pois corriqueiramente as manutenções realizadas derivam de suporte técnico demandado, ou que demandam suporte técnico para sua correta implantação.

**6.3.** Não há viabilidade para formação de consórcios, visto que a estrutura da solução é única, não cabendo tal formação para fornecimento de objeto uno e indivisível.

## 7. NECESSIDADES DE ADEQUAÇÃO DO AMBIENTE (Decreto n. 15./477/2020, Art. 8°, VII)

**7.1.** Não foram identificadas necessidades de adequação do ambiente para execução contratual, em relação ao modelo que já é adotado.

## 8. ESTIMATIVAS DO CUSTO TOTAL DA CONTRATAÇÃO (Decreto n. 15./477/2020, Art. 8°, VIII)

**8.1.** A definição e documentação da estimativa de preços referenciais foram baseadas nas seguintes premissas:

a) Preços praticados no contrato de prestação de serviços do contrato n° 001/2019, GCONT n° 11458 (Pregão Eletrônico n° 007/2018 - SEFAZ, processo n° 11/018.316/2018;

b) Preços praticados no contrato de prestação de serviços do contrato nº 033/DPGE/2017, (Pregão Eletrônico nº 000012/2017, da Defensoria Pública de Mato Grosso do Sul);

**8.2.** A concretização da pesquisa de preços e memórias de cálculo resultou nos seguintes valores:

8.2.1. O valor estimado mensal da presente contratação é de R$ 133.750,00 (cento e trinta e três mil e setecentos e cinquenta reais).

8.2.2. O valor estimado global da presente contratação é de R$ R$ 1.605.000,00 (um milhão seiscentos e cinco mil reais).

**8.3.** A planilha de composição de custos unitários da Solução de Tecnologia da Informação e Comunicação conforme abaixo:

| CONTRATO | EMPRESA | UNID. | QTDE | VL. UNITÁRIO | VL. TOTAL |
|---|---|---|---|---|---|
| 001/2019 | IMAGETECH TECNOLOGIA EM INFORMÁTICA LTDA | MÊS | 12 | R$ 118.500,00 | R$ 1.422.000,00 |
| 033/DPGE/ 2017 | DEFENSORIA PÚBLICA DE MATO GROSSO DO SUL | MÊS | 12 | R$ 149.000,00 | R$ 1.788.000,00 |
| **VALOR GLOBAL** | | | | | **R$ 1.605.000,00** |

**8.4.** A planilha de composição de custos unitários da Solução de Tecnologia da Informação e Comunicação estará presente em Anexo ao Termo de Referência.

## 9. ANÁLISE DE RISCOS (Decreto n. 15./477/2020, Art. 8°, § 1°)

**9.1.** Riscos do processo de contratação e gestão contratual:

| **Risco 01** | **Problemas no processo de licitação para contratação** | |
|---|---|---|
| **Probabilidade** | Alta | |
| **Id.** | **Dano** | **Impacto** |
| 1. | Atraso no processo de contratação. | Alto |
| **Id.** | **Ação Preventiva** | **Responsável** |
| 1. | Cumprimento dos prazos para contratação, revisar e acompanhar as mudanças nos documentos de planejamento da contratação que influenciam no descumprimento do cronograma. | Equipe de Planejamento da Contratação |
| 2. | Elaborar os documentos de planejamento da contratação com estrita observância à legislação e normativos complementares. | Equipe de Planejamento da Contratação |
| **Id.** | **Ação de Contingência** | **Responsável** |
| 1. | Dedicação exclusiva da equipe de planejamento para minimizar os impactos. | Equipe de Planejamento da Contratação |

| **Risco 02** | **Contingenciamento orçamentário** | |
|---|---|---|
| **Probabilidade** | Alta | |
| **Id.** | **Dano** | **Impacto** |
| 1. | Descontinuidade dos serviços. | Alto |
| 2. | Redução da qualidade dos serviços entregues. | Alto |
| **Id.** | **Ação Preventiva** | **Responsável** |
| 1. | Verificar outras possibilidades de orçamento para realizar a contratação. | Equipe de Planejamento da Contratação |
| | Demonstrar a necessidade e a relevância do contrato para manutenção e/ou sustentação dos serviços públicos. | Gestor do Contrato |

| Id. | Ação de Contingência | Responsável |
|---|---|---|
| 1. | Demonstrar claramente à alta gestão a importância da contratação. | Equipe de Planejamento da Contratação |
| 2. | Caso seja extremamente necessário o contingenciamento no contrato, Identificar os pontos que causarão menor impacto caso sejam suprimidos. | Gestor do Contrato |

| Risco 03 | Falha na caracterização do objeto | |
|---|---|---|
| Probabilidade | Baixa | |
| Id. | Dano | Impacto |
| 1. | Não atendimento das necessidades da contratação. | Alto |
| 2. | Rescisão contratual | Alto |
| 3. | Descontinuidade dos Serviços | Alto |
| Id. | Ação Preventiva | Responsável |
| 1. | Definir requisitos técnicos alinhados às necessidades do negócio e aos objetivos da contratação. | Equipe de Planejamento da Contratação |
| 2. | Revisar os artefatos de planejamento da contratação para avaliar se atendem às necessidades e aos objetivos propostos. | Equipe de Planejamento da Contratação |
| Id. | Ação de Contingência | Responsável |
| 1. | Corrigir os artefatos de planejamento da contratação para resolver as falhas identificadas. | Equipe de Planejamento da Contratação |
| 2. | Aperfeiçoar a elaboração dos documentos de planejamento da contratação detalhando minuciosamente as características do objeto da contratação. | Equipe de Planejamento da Contratação |

| Risco 04 | Falha na justificativa para escolha da solução | |
|---|---|---|
| Probabilidade | Baixa | |
| Id. | Dano | Impacto |
| 1. | Não atendimento ao princípio da motivação dos atos administrativos. | Alto |
| 2. | Impossibilidade de contratação. | Alto |
| Id. | Ação Preventiva | Responsável |
| 1. | Justificar a necessidade dos requisitos técnicos exigidos, alinhando-se às necessidades da contratação, principalmente quando implicarem em redução da competitividade do processo seleção do fornecedor. | Equipe de Planejamento da Contratação |
| 2. | Avaliar se os requisitos exigidos são os estritamente necessários e justificáveis para o atendimento das expectativas da contratação proposta. | Equipe de Planejamento da Contratação |
| Id. | Ação de Contingência | Responsável |
| 1. | Justificar a necessidade perante órgãos de controle. | Equipe de Planejamento da Contratação |
| 2. | Caso seja negada a continuidade da contratação, instituir nova equipe de planejamento da contratação e promover uma nova contratação | Autoridade Superior da UG |
| 3. | Aperfeiçoar a elaboração dos documentos de planejamento da contratação exigindo apenas os requisitos estritamente necessários e justificáveis para | Equipe de Planejamento da Contratação |

| | | |
|---|---|---|
| | o atendimento das expectativas da contratação proposta. | |

| **Risco 05** | **Restrição à competitividade** | |
|---|---|---|
| **Probabilidade** | Baixa | |
| **Id.** | **Dano** | **Impacto** |
| 1. | Elevação do preço da contratação. | Alto |
| 2. | Suspensão da contratação. | Alto |
| 3. | Direcionamento indevido do objeto. | Alto |
| **Id.** | **Ação Preventiva** | **Responsável** |
| 1. | Evitar a inclusão de requisitos excessivos e que restringem a competitividade, se atentando apenas aos requisitos estritamente necessários para atender o objetivo da contratação. | Equipe de Planejamento da Contratação |
| 2. | Avaliar se os requisitos exigidos são os estritamente necessários e justificáveis para o atendimento das expectativas da contratação proposta. | Equipe de Planejamento da Contratação |
| **Id.** | **Ação de Contingência** | **Responsável** |
| 1. | Supressão dos critérios restritivos. | Equipe de Planejamento da Contratação |
| 2. | Aperfeiçoar a elaboração dos documentos de planejamento da contratação exigindo apenas os requisitos estritamente necessários e justificáveis para o atendimento das expectativas da contratação proposta. | Equipe de Planejamento da Contratação |

| **Risco 06** | **Falha na pesquisa de preços** | |
|---|---|---|
| **Probabilidade** | Médio | |
| **Id.** | **Dano** | **Impacto** |
| 1. | Elevação dos preços ou inexequibilidade das propostas. | Alto |
| 2. | Impossibilidade de contratação. | Alto |
| **Id.** | **Ação Preventiva** | **Responsável** |
| 1. | Seguir os procedimentos normatizados para a realização de pesquisa de preços. | Equipe de Planejamento da Contratação |
| 2. | Ampliar a pesquisa de preços, não se restringindo a apenas três propostas. | Equipe de Planejamento da Contratação |
| 3. | Avaliar se os procedimentos adotados estão de acordo com os requisitos normativos. | Unidade Administrativa da UG |
| 4. | Levar em consideração os questionamentos das empresas concorrentes. | Equipe de Planejamento da Contratação |
| **Id.** | **Ação de Contingência** | **Responsável** |
| 1. | Refazer a pesquisa de preços precedidas de uma consulta pública para esclarecimentos ou correção de distorções. | Equipe de Planejamento da Contratação |

| **Risco 07** | **Impugnações ou interposição de recurso** | |
|---|---|---|
| **Probabilidade** | Alta | |
| **Id.** | **Dano** | **Impacto** |
| 1. | Atraso no processo de contratação. | Alto |
| 2. | Suspensão da contratação. | Alto |

| | | |
|---|---|---|
| 3. | Impossibilidade de contratação. | Alto |
| **Id.** | **Ação Preventiva** | **Responsável** |
| 1. | Elaborar e revisar criteriosamente os artefatos de planejamento da contratação de acordo com os normativos vigentes. | Equipe de Planejamento da Contratação |
| 2. | Avaliar e realizar os ajustes recomendados pela Consultoria Jurídica para sanar inconformidades dos documentos de planejamento da contratação com a legislação vigente. | Equipe de Planejamento da Contratação |
| **Id.** | **Ação de Contingência** | **Responsável** |
| 1. | Empenhar-se no atendimento aos pedidos de esclarecimento buscando nos repositórios legais e jurisprudenciais os elementos de sustentação das opções adotadas para a contratação. | Equipe de Planejamento da Contratação |
| 2. | Caso seja negada a continuidade da contratação, instituir nova equipe de planejamento da contratação e promover uma nova contratação. | Autoridade Superior da UG |
| 3. | Aperfeiçoar a elaboração dos documentos de planejamento da contratação com estrita observância à legislação e normativos complementares. | Equipe de Planejamento da Contratação |

| **Risco 08** | **Descumprimento de cláusulas contratuais pela Contratada** | |
|---|---|---|
| **Probabilidade** | Média | |
| **Id.** | **Dano** | **Impacto** |
| 1. | Não entrega dos serviços e equipamentos. | Alto |
| 2. | Atraso na entrega dos serviços e equipamentos. | Alto |
| 3. | Baixa qualidade dos serviços e equipamentos entregues. | Alto |
| 4. | Descontinuidade dos serviços. | Alto |
| 5. | Falta de efetividade da contratação. | Alto |
| **Id.** | **Ação Preventiva** | **Responsável** |
| 1. | Acompanhar a execução dos serviços aferindo se os requisitos exigidos no contrato estão sento cumpridos de acordo com a qualidade exigida. | Fiscal e Gestor do Contrato |
| 2. | Avaliar se os serviços prestados estão atendendo as expectativas da contratação. | Fiscal e Gestor do Contrato |
| 3. | Dimensionamento adequado do corpo de fiscalização e gestão contratual. | Autoridade Superior da UG |
| 4. | Capacitação de equipe de fiscalização e gestão contratual. | Autoridade Superior da UG |
| 5. | Intensificação no processo de fiscalização e gestão contratual | Fiscal e Gestor do Contrato |
| **Id.** | **Ação de Contingência** | **Responsável** |
| 1. | Notificar formalmente a Contratada quando cláusulas do contrato forem descumpridas. | Fiscal e Gestor do Contrato |
| 2. | Aplicar glosas e penalidades previstas no instrumento convocatório, de forma a coibir a reincidência. | Fiscal e Gestor do Contrato |
| 3. | Instituir nova equipe de planejamento da contratação e promover uma nova contratação para evitar o comprometimento da continuidade dos serviços sustentados pela solução de TIC, em caso de | Autoridade Superior da UG |

| | | |
|---|---|---|
| | dificuldade de resolução das inconformidades. | |

| **Risco 09** | **Irregularidade no cumprimento de questões trabalhistas** | |
|---|---|---|
| **Probabilidade** | Média | |
| **Id.** | **Dano** | **Impacto** |
| 1. | Desmotivação dos profissionais prestadores de serviços. | Alto |
| 2. | Aumento da rotatividade dos profissionais. | Médio |
| 3. | Baixa qualidade dos serviços entregues. | Alto |
| 4. | Corresponsabilização de equipe de gestão e fiscalização. | Alto |
| 5. | Descontinuidade dos serviços. | Alto |
| **Id.** | **Ação Preventiva** | **Responsável** |
| 1. | Elaborar lista de verificação que deverá ser observada pela fiscalização administrativa, durante a execução do contrato. | Fiscal e Gestor do contrato |
| 2. | Realizar a fiscalização do cumprimento das obrigações trabalhistas, conforme legislação vigente. | Fiscal e Gestor do contrato |
| **Id.** | **Ação de Contingência** | **Responsável** |
| 1. | Notificar formalmente a Contratada quando forem identificadas irregularidades trabalhistas. | Fiscal e Gestor do Contrato |
| 2. | Aplicar glosas e penalidades previstas no instrumento convocatório. | Fiscal e Gestor do Contrato |
| 3. | Instituir nova equipe de planejamento da contratação e promover uma nova contratação para evitar o comprometimento da continuidade dos serviços sustentados pela Solução de TIC. | Autoridade Superior da UG |

| **Risco 10** | **Vazamento de dados e informações pelos funcionários da Contratada** | |
|---|---|---|
| **Probabilidade** | Alta | |
| **Id.** | **Dano** | **Impacto** |
| 1. | Divulgação de informações privilegiadas e restritas. | Alto |
| 2. | Quebra de confidencialidade de dados, informações e documentos | Alto |
| 3. | Redução da credibilidade do órgão/entidade. | Alto |
| **Id.** | **Ação Preventiva** | **Responsável** |
| 1. | Exigir dos funcionários da Contratada assinatura de Termo de Compromisso de obediência às normas de segurança e Sigilo do órgão/entidade. | Fiscal e Gestor do Contrato |
| 2. | Estabelecer o Gerenciamento de Configuração e Ativo de Serviço para controlar os recursos computacionais, incluindo a concessão de acesso aos recursos. | Unidade de Tecnologia da Informação da UG |
| 3. | Manter a Contratada e seus profissionais cientes e da Política de Segurança da Informação. | Fiscal e Gestor do Contrato |
| 4. | Estabelecer, conscientizar e divulgar os procedimentos de controle de permissões e perfis de acesso, principalmente para terceiros que podem ter alta rotatividade. | Unidade de Tecnologia da Informação da UG |
| **Id.** | **Ação de Contingência** | **Responsável** |
| 1. | Aplicar sanções administrativas, cíveis e criminais | Unidade Administrativa e/ou Jurídica da UG |

| | | |
|---|---|---|
| 2. | Exigir reparação do dano, quando aplicável. | Unidade Administrativa e/ou Jurídica da UG |

| **Risco 11** | **Alta rotatividade de funcionários da Contratada** | |
|---|---|---|
| **Probabilidade** | Média | |
| **Id.** | **Dano** | **Impacto** |
| 1. | Ingressos frequentes de mais pessoas estranhas à organização. | Alto |
| 2. | Falta de conhecimento do ambiente e integração com os demais colaboradores. | Alto |
| **Id.** | **Ação Preventiva** | **Responsável** |
| 1. | Determinar de forma precisa e clara as especificações técnicas do contrato bem como os requisitos de qualificação técnica dos colaboradores da Contratada, definindo as atividades, papéis e responsabilidades com vistas a possibilitar a transparência e a vantajosidade técnica e econômica da licitação. | Equipe de Planejamento da Contratação |
| **Id.** | **Ação de Contingência** | **Responsável** |
| 1. | Promover ações de construção, manutenção e atualização das bases de conhecimento, de modo a facilitar a substituição de técnicos. | Equipe de Fiscalização do Contrato |

| **Risco 12** | **Custo do objeto licitado superior ao estimado para a contratação dos serviços** | |
|---|---|---|
| **Probabilidade** | Baixa | |
| **Id.** | **Dano** | **Impacto** |
| 1. | Comprometimento da economicidade da contratação. | Alto |
| 2. | Não adjudicação do objeto. | Alto |
| **Id.** | **Ação Preventiva** | **Responsável** |
| 1. | Revisar as estimativas dos custos estimados do estudo técnico. | Equipe de Planejamento da Contratação |
| **Id.** | **Ação de Contingência** | **Responsável** |
| 1. | Não havendo possibilidade de redução dos valores negociados, deve-se suspender o certame com vistas redefinição de escopo do objeto e do processo de Planejamento da Contratação. | Autoridade Superior da UG |

| **Risco 13** | **Atraso no processo de contratação da solução** | |
|---|---|---|
| **Probabilidade** | Alta | |
| **Id.** | **Dano** | **Impacto** |
| 1. | Descontinuidade dos serviços de infraestrutura de TI. | Alto |
| 2. | Comprometimento dos serviços prestados. | Alto |
| **Id.** | **Ação Preventiva** | **Responsável** |
| 1. | Cumprimento dos prazos para contratação, revisar e acompanhar as mudanças nos documentos de planejamento da contratação que influenciam no descumprimento do cronograma. | Equipe de Planejamento da Contratação |
| 2. | Elaborar os documentos de planejamento da contratação com estrita observância à legislação e normativos complementares. | Equipe de Planejamento da Contratação |
| **Id.** | **Ação de Contingência** | **Responsável** |
| 1. | Dedicação exclusiva da equipe de planejamento para | Equipe de Planejamento da |

| | | |
|---|---|---|
| | minimizar os impactos. | Contratação |
| 2. | Renovação do contrato de suporte e garantia com a atual Contratada por mais 12 meses com a possibilidade de rescisão contratual por parte da Contratante a qualquer momento. | Autoridade Superior da UG |

**9.2.** Riscos que comprometem a Solução de Tecnologia da Informação e Comunicação

| **Risco 01** | **Interrupção da execução contratual ou rescisão do contrato** | |
|---|---|---|
| **Probabilidade** | Média | |
| **Id.** | **Dano** | **Impacto** |
| 1. | Descontinuidade dos serviços sustentados pela STIC. | Alto |
| 2. | Comprometimento dos serviços prestados pela UG. | Alto |
| **Id.** | **Ação Preventiva** | **Responsável** |
| 1. | Acompanhar a execução dos serviços aferindo criteriosamente se os requisitos estão sento cumpridos de acordo com a qualidade exigida, buscando identificar qualquer problema de execução em sua origem para não permitir maiores impactos no contrato. | Fiscal e Gestor do Contrato |
| 2. | Avaliar se os serviços prestados estão atendendo as expectativas da contratação. | Fiscal e Gestor do Contrato |
| 3. | Garantir que o conhecimento seja repassado continuamente para a equipe de fiscalização técnica. | Fiscal e Gestor do Contrato |
| 4. | Executar atividades de validação do ambiente (verificação de Alta disponibilidade, atualização do equipamento, dentre outras.) | Unidade de Tecnologia da Informação da UG |
| **Id.** | **Ação de Contingência** | **Responsável** |
| 1. | Iniciar novo processo de contratação, utilizando os artefatos de planejamento produzidos, com as atualizações baseadas na Infraestrutura e experiência adquirida no processo de gestão e fiscalização. | Autoridade Superior da UG |

| **Risco 02** | **Falta de pessoal técnico competente para fiscalização do contrato** | |
|---|---|---|
| **Probabilidade** | Alta | |
| **Id.** | **Dano** | **Impacto** |
| 1. | Deficiência na fiscalização do contrato com comprometimento na aferição dos níveis de serviço. | Alto |
| 2. | Baixa qualidade nas entregas dos serviços. | Alto |
| 3. | Não atendimento das expectativas da contratação. | Alto |
| 4. | Atrasos no pagamento, pagamento indevido e sem o devido desconto das glosas. | Alto |
| 5. | Inexecução parcial ou total do contrato. | Alto |
| **Id.** | **Ação Preventiva** | **Responsável** |
| 1. | Definir indicadores de fácil mensuração e que podem ser monitorados por meio da ferramenta de gestão de serviços de TIC. | Equipe de Planejamento da Contratação |
| 2. | Elaborar Plano de Fiscalização prevendo como deverá ser realizada a fiscalização do contrato, incluindo modelos de planilhas de aferição e listas de verificação. | Equipe de Planejamento da Contratação |
| 3. | Identificar se existem servidores com habilidades e competências em TIC adequadas e em quantidade | Equipe de Planejamento da Contratação |

| | | |
|---|---|---|
| | suficiente para a atuação na fiscalização dos serviços contratados e mensuração sistemática dos indicadores e da qualidade dos serviços. | |
| 4. | Promover o recrutamento de servidores públicos, de outras áreas ou outros órgãos, que possuam habilidades e competências em TIC adequadas para a aferição sistemática da qualidade das entregas dos serviços contratados. | Autoridade Superior da UG |
| 5. | Propor processo de seleção de servidores públicos, afim de alocar servidores que possuem competências técnicas adequadas para a aferição sistemática das entregas dos serviços contratados. | Autoridade Superior da UG |
| **Id.** | **Ação de Contingência** | **Responsável** |
| 1. | Primar pela demanda de atividades críticas, que envolvam a disponibilidade do ambiente tecnológico | Fiscal e Gestor do Contrato |
| 2. | Propor processo seletivo simplificado para contratação de servidores temporários com habilidades e competências em TIC adequadas para a aferição sistemática da qualidade das entregas dos serviços contratados. | Autoridade Superior da UG |

| **Risco 03** | **Prestação de serviço por profissionais inexperientes ou sem conhecimento técnico adequado** | |
|---|---|---|
| **Probabilidade** | Média | |
| **Id.** | **Dano** | **Impacto** |
| 1. | Baixa qualidade nas entregas dos serviços. | Alto |
| 2. | Atraso na entrega dos serviços. | Médio |
| 3. | Indisponibilidade de serviços críticos. | Alto |
| 4. | Descumprimento dos requisitos contratuais. | Alto |
| **Id.** | **Ação Preventiva** | **Responsável** |
| 1. | Prever requisitos de qualificação técnica e experiência profissional de acordo com complexidade de cada tipo de serviço. | Equipe de Planejamento da Contratação |
| 2. | Realizar a fiscalização do cumprimento dos requisitos de qualificação técnica e experiência profissional exigidos. | Fiscal e Gestor do Contrato |
| **Id.** | **Ação de Contingência** | **Responsável** |
| 1. | Notificar formalmente a Contratada quando os requisitos do contrato não forem descumpridos. | Fiscal e Gestor do Contrato |
| 2. | Aplicar glosas e penalidades previstas no instrumento convocatório, de forma a coibir a reincidência. | Fiscal e Gestor do Contrato |

| **Risco 04** | **Não atendimento dos Níveis Mínimos de Serviços** | |
|---|---|---|
| **Probabilidade** | Alta | |
| **Id.** | **Dano** | **Impacto** |
| 1. | Não atendimento aos requisitos de negócio. | Alto |
| 2. | Ineficiência e não efetividade da contratação | Alto |
| **Id.** | **Ação Preventiva** | **Responsável** |
| 1. | Prever sanções pelo descumprimento dos Níveis Mínimos de Serviços. | Equipe de Planejamento da Contratação |
| 2. | Estabelecer meios de monitoração e controle proativos da qualidade dos serviços. | Equipe de Planejamento da Contratação |

| | | |
|---|---|---|
| 3. | Atuar proativamente e continuamente na aferição da qualidade dos serviços executados intervindo nos desvios de qualidade. | Fiscal e Gestor do Contrato |
| **Id.** | **Ação de Contingência** | **Responsável** |
| 1. | Realizar as intervenções que forem necessárias para o reestabelecimento imediato do atendimento e dos serviços. | Fiscal e Gestor do Contrato |
| 2. | Notificar formalmente a Contratada quando cláusulas do contrato forem descumpridas ou violadas. | Fiscal e Gestor do Contrato |
| 3. | Aplicar glosas e penalidades previstas no instrumento convocatório, de forma a coibir a reincidência. | Unidade Administrativa e/ou Jurídica da UG |

| **Risco 05** | **Falha na estimativa de volume de serviços** | |
|---|---|---|
| **Probabilidade** | Alta | |
| **Id.** | **Dano** | **Impacto** |
| 1. | Não atendimento das expectativas da contratação. | Alto |
| 2. | Superdimensionamento ou subdimensionamento do contrato. | Alto |
| 3. | Contratação antieconômica e sobrepreço. | Alto |
| 4. | Rescisão contratual. | Alto |
| **Id.** | **Ação Preventiva** | **Responsável** |
| 1. | Realizar o levantamento criterioso do volume de serviços executados antes da contratação para estimar adequadamente o volume previsto. | Equipe de Planejamento da Contratação |
| 2. | Elaboração minuciosa da memória de cálculo. | Equipe de Planejamento da Contratação |
| **Id.** | **Ação de Contingência** | **Responsável** |
| 1. | Solicitar aditivo de acréscimo ou supressão contratual. | Gestor do Contrato |
| 2. | Instituir nova equipe de planejamento da contratação e promover uma nova contratação para evitar o comprometimento da continuidade dos serviços sustentados pela STIC. | Autoridade Superior da UG |

| **Risco 06** | **Descumprimento de cláusulas contratuais pela Contratada** | |
|---|---|---|
| **Probabilidade** | Alta | |
| **Id.** | **Dano** | **Impacto** |
| 1. | Não entrega dos serviços. | Alto |
| 2. | Atraso na entrega dos serviços | Alto |
| 3. | Entrega com qualidade inferior à exigida | Alto |
| **Id.** | **Ação Preventiva** | **Responsável** |
| 1. | Definição de níveis de serviços adequados | Equipe de Planejamento da Contratação |
| 2. | Acompanhamento e verificação de qualidade do serviço prestado | Fiscal e Gestor do Contrato |
| **Id.** | **Ação de Contingência** | **Responsável** |
| 1. | Aplicação de glosas e, caso haja prejuízo maior previsto nos níveis mínimos de serviço, aplicação das sanções cabíveis, de forma a coibir a reincidência | Fiscal e Gestor do Contrato |

| **Risco 07** | **Indisponibilidade dos serviços de TI por não atendimento das demandas nos prazos definidos** |
|---|---|

| Probabilidade | Média | |
|---|---|---|
| **Id.** | **Dano** | **Impacto** |
| 1. | Paralisação dos serviços de infraestrutura de TI e indisponibilidade dos sistemas críticos | Alto |
| 2. | Comprometimento dos serviços prestados | Alto |
| **Id.** | **Ação Preventiva** | **Responsável** |
| 1. | Prever sanções pelo descumprimento dos Níveis Mínimos de Serviços | Equipe de Planejamento da Contratação |
| 2. | Estabelecer meios de monitorar e controlar a qualidade dos serviços prestados | Equipe de Planejamento da Contratação |
| 3. | Atuar de forma proativa e contínua na aferição da qualidade dos serviços | Fiscal e Gestor do Contrato |
| 4. | Prover e implementar recursos e tecnologias de alta disponibilidade | Fiscal e Gestor do Contrato |
| **Id.** | **Ação de Contingênca** | **Responsável** |
| 1. | Aplicação de glosas e, caso haja prejuízo maior previsto nos níveis mínimos de serviço, aplicação das sanções cabíveis, de forma a coibir a reincidência | Unidade Administrativa e/ou Jurídica da UG |

## 10. DECLARAÇÃO DA VIABILIDADE OU NÃO DA CONTRATAÇÃO (Decreto n. 15.477/2020, Art. 8°, IX)

**10.1.** Conforme fundamentação acima, esta Equipe de Planejamento da Contratação considera que a Solução de Tecnologia da Informação e Comunicação escolhida é viável, com base nos elementos anteriormente apresentados neste Estudo Técnico Preliminar, além de ser necessária para o atendimento das necessidades e interesses do SGI/SEFAZ.

**10.2.** A contratação obedece às disposições do Decreto Estadual n. 15.477 de 20 de julho de 2020 e está em harmonia com o Planejamento Estratégico Estadual.

## 11. ASSINATURAS

_____

**GUSTAVO NANTES GUALBERTO**
**ASSESSOR TÉCNICO**
**SGI/SEFAZ/MS**

_____

**CELSO TADASHI TANAKA**
**COORDENADOR**
**SGI/SEFAZ/MS**

Aprovado em: _____ / _____ / _____

_____

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