Serviço Municipal de Águas e Esgotos
Rua Otto Unger, 450 - Centro
CEP 08780-908 - Mogi das Cruzes – SP
(11) 4798-5105

TERMO DE REFERÊNCIA FIREWALL

SUMÁRIO

1. DO OBJETO

1.1. Contratação de solução de segurança do acesso à *internet*, com alta disponibilidade do tipo *Firewall Next Generation Firewall* (*NGFW*) - *APPLIANCE* modelo NSA 2700, do fabricante *Sonicwall*, compreendendo equipamentos físicos, componentes, *software*, serviços especializados de instalação, implantação, configuração, treinamento e suporte técnico continuado.

1.2. DETALHAMENTO DO OBJETO

1.2.1. O SEMAE dispõe em seu *datacenter* de uma solução de acesso à *internet*, também chamada de segurança de rede, que compreende as funcionalidades de *firewall*, filtro de conteúdo, *IPS*, balanceador de carga antivírus de borda e *AntiSpam*, do fabricante *Sonicwall* modelo NSA2600;

1.2.2. De forma a manter a padronização e qualidade do ambiente de acesso à *internet* do SEMAE, se faz necessária a substituição e atualização do *firewall* para o modelo *Sonicwall* NSA2700, dada a descontinuação do suporte e manutenção para *hardware* e *software* do fabricante para o modelo em uso pelo SEMAE, o NSA2600.

1.3. FUNDAMENTAÇÃO E JUSTIFICATIVA PARA DEFINIÇÃO DA MARCA E MODELO

1.3.1. Em 2015, o SEMAE adquiriu a solução de segurança de redes, por meio do processo licitatório tipo pregão de número 034/2015, através do processo administrativo de número 2015/204049. A solução vencedora foi do fabricante *Sonicwall* que foi entregue, instalada e configurada no equipamento *firewall* modelo NSA2600, ativa até o presente momento;

1.3.2. Estas soluções vêm se mostrando robustas e eficientes na proteção do acesso à *internet* da instituição sendo um importante componente de segurança da informação;

1.3.3. Os equipamentos, os *softwares* e serviços deste Termo de Referência visam amadurecer a solução existente no SEMAE;

1.3.4. Foram descritos neste termo a marca e modelo dos equipamentos e *softwares* necessários. Tal definição é necessária para manter a compatibilidade e correto funcionamento da solução existente;

1.3.5. A definição da marca de modelo supra citadas não impede que soluções de segurança do acesso à *internet* de outros fabricantes, de características superiores, sejam oferecidas.

1.4. ESPECIFICAÇÃO TÉCNICA DO SERVIÇO DE SEGURANÇA DO ACESSO À INTERNET

1.4.1. **SERVIÇO DE PROTEÇÃO CONTRA AMEAÇAS DA *INTERNET***

1.4.1.1. Para as ameaças de dia-zero, a solução deve ter a habilidade de prevenir o ataque antes de qualquer assinatura ser criada. Deve possuir módulo de antivírus e *Anti-Bot* integrado ao próprio *appliance* de segurança.

1.4.1.2. A solução de antivírus integrada deve ter capacidade de analisar arquivos maiores que 1 *Gigabytes* (GB);

1.4.1.3. 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.

1.4.1.4. 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.

1.4.1.5. Implementar funcionalidade de detecção e bloqueio de *call-backs*.

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

1.4.1.7. A solução *Anti-bot* deve possuir mecanismo de detecção que inclua reputação de endereço IP.

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

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

1.4.1.10. Deve possuir visualização na própria interface de gerenciamento dos incidentes mais ocorridos com *hosts*, vírus e/ou *Bots*;

1.4.1.11. Permitir o bloqueio de *malwares* (vírus, *worms*, *spyware* e etc.)

1.4.1.12. A solução deve ser capaz de proteger contra ataques a *DNS*.

1.4.1.13. A solução deve ser capaz de prevenir acesso a *websites* maliciosos.

1.4.1.14. A solução deverá receber atualizações de um serviço baseado em *cloud*.

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

1.4.1.16. A solução antivírus deverá suportar análise de arquivos que trafegam dentro do protocolo *CIFS*;

1.4.1.17. A solução deve suportar funcionalidade de *Geo-IP*, entregando 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

1.4.1.18. Deve possuir proteção *anti-spoofing*;

1.4.1.19. Possuir assinaturas específicas, ou implementar mecanismo interno no *appliance*, para mitigação de ataques *DoS (Denial-of-service)* e *DDoS (Distributed DoS*);

1.4.1.20. Ser imune e capaz de impedir ataques conhecidos à camada *Open Systems Interconnection* (OSI);

1.4.1.21. Detectar e bloquear a origem de *portscans*.

1.4.1.22. Deve permitir o bloqueio de ataques

1.4.1.23. Deve permitir o bloqueio de *exploits* conhecidos divulgados em listas de distribuições como https://cvexploits.io/, https://www.cisa.gov/, https://www.cve.org/ ou alguma lista mantida pelo fabricante da solução;

1.4.1.24. O *gateway* antivírus deve suportar a análise de pelo menos os protocolos *HTTP, FTP, IMAP* e *SMTP.*

1.4.2. **SERVIÇO DE PROTEÇÃO CONTRA ATAQUES AVANÇADOS**

1.4.2.1. Deverá prover as funcionalidades de inspeção de tráfego de entrada e saída de *malwares* não conhecidos ou do tipo ATP (*Advanced Threat Protection*), com filtro de ameaças avançadas e análise de execução em tempo real, e inspeção de tráfego de saída de *call-backs;*

1.4.2.2. Suportar os protocolos *HTTP* e a inspeção de tráfego criptografado *HTTPS*.

1.4.2.3. A solução deve ser capaz de inspecionar o tráfego criptografado *SSL/TLS* e *SSH*.

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

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

1.4.2.6. 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.

1.4.2.7. Implementar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional *Windows*, *Linux* e *Android*.

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

1.4.2.9. 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.

1.4.2.10. A solução deve possuir nuvem de inteligência proprietária do fabricante, onde este seja responsável por atualizar toda a base de segurança dos *appliance* através de assinaturas.

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

1.4.2.12. Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e quaisquer outros mecanismos de redirecionamento de tráfego;

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

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

1.4.2.15. 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.

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

1.4.2.17. Implementar a análise de arquivos executáveis, *DLLs* e *ZIP* no ambiente controlado.

1.4.2.18. Mitigar ameaças de dia zero de forma transparente para o usuário final.

1.4.2.19. Mitigar ameaças de dia zero através de tecnologias de emulação e código de registro.

1.4.2.20. Implementar mecanismo de pesquisa por diferentes intervalos de tempo.

1.4.2.21. Mitigar ameaças de dia zero via tráfego de *internet*.

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

1.4.2.23. Mitigar ameaças de dia zero que possam burlar o sistema operacional emulado.

1.4.2.24. A solução deve permitir a criação de listas brancas (*whitelist*) baseadas no *MD5* do arquivo.

1.4.2.25. Mitigar ameaças de dia zero antes da execução e evasão de qualquer código malicioso.

1.4.2.26. Conter e mitigar *exploits* avançados.

1.4.2.27. A análise em nuvem 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 *Anti-Spyware* automaticamente, definir *URLs* não confiáveis utilizadas pelo novo *malware* e prover informações sobre o usuário infectado (seu endereço *IP* e seu login de rede).

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

1.4.3. **SERVIÇO DE *VITUAL PRIVATE NETWORK* (*VPN*) SEGURA**

1.4.3.1. 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*;

1.4.3.2. Suportar, no mínimo, estes algoritmos de criptografia: 3DES, AES 128 e AES 256;

1.4.3.3. Suportar, no mínimo, estes algoritmos *Hash*: SHA-256 e SHA-384

1.4.3.4. Suporte para o *Diffie-Hellman* grupo 2 (1024 *bits*), grupo 5 (1536 *bits*) e grupo 14 (2048 *bits*).

1.4.3.5. Deverá suportar algoritmo *Internet Key Exchange* (*IKE*)v1 e v2

1.4.3.6. Suporte para autenticação via de túneis *IPSec* via certificado digital para *VPNs Site-to-Site* e *Client-to-Site*

1.4.3.7. A solução deve suportar *VPNs L2TP*, incluindo suporte para *Apple iOS* e *Android*.

1.4.3.8. Solução deve suportar *VPNs* baseadas em políticas, e *VPNs* baseadas em roteamento estático e/ou dinâmico.

1.4.3.9. 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*;

1.4.3.10. Deve incluir a capacidade de estabelecer *VPNs* com outros *firewalls* que utilizam *IP* públicos dinâmicos.

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

1.4.3.12. Permitir criação de políticas de roteamento estático 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.

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

1.4.3.14. Implementar os esquemas de troca de chaves manual, *IKE* e *IKEv2* por *Pre-Shared Key* (*PSK*), certificados digitais e *XAUTH client authentication*;

1.4.3.15. Deve possuir interoperabilidade, no mínimo, com os seguintes fabricantes: *Cisco*, *Check Point*, *Juniper*, *Palo Alto Networks*, *Fortinet* e *SonicWall;*

1.4.3.16. A *VPN Client-to-Site IPsec* deve ser licenciada para, no mínimo, 50 usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para, no mínimo, 1000 usuários simultâneos, com aquisição de licença complementar;

1.4.3.17. A *VPN SSL* deve ser licenciada para, no mínimo, 10 usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para, no mínimo, 500 usuários simultâneos, com aquisição de licença complementar.

1.4.3.18. Deve suportar 2000 túneis de *VPN tipo Site-to-Site* padrão *IPSEC* simultâneos

1.4.3.19. Deve suportar, no mínimo, 2.1 Gbps de desempenho de *VPN IPSEC*.

1.4.4. **SERVIÇO DE ACESSO À INTERNET E CARACTERÍSTICAS DE AUTENTICAÇÃO**

1.4.4.1. Implementar *proxy* transparente para o protocolo *HTTP*, de forma a dispensar a configuração dos navegadores das máquinas clientes;

1.4.4.2. Possuir servidor de *DHCP* (*Dynamic Host Configuration Protocol*) interno com capacidade de alocação de endereçamento *IP* para as estações conectadas às interfaces do *firewall* e via *VPN*;

1.4.4.3. Deve suportar *DHCP relay*;

1.4.4.4. Possibilitar a aplicação de regras de *firewall* e *IPS* por *IP* e grupo de usuários, permitindo a definição de regras para determinado horário ou período (dia da semana e hora) com matriz de horários que possibilite o bloqueio de serviços em horários específicos, tendo o início e fim das conexões vinculadas a essa matriz de horários;

1.4.4.5. Deve permitir a utilização de regras de antivírus, *Anti-Spyware*, *IPS* e filtro de conteúdo *web* por segmentos de rede. Todos os serviços devem ser suportados no mesmo segmento de rede, *VLAN* ou zona de segurança;

1.4.4.6. Possuir capacidade de inspecionar e bloquear, em tempo real, aplicativos de transferências de arquivos, softwares *P2P* (*Peer-to-Peer*) incluindo, no mínimo, os *softwares Kazaa*, *Limewire*, *Morpheus* e *Napster*, e *softwares* comunicadores instantâneos (*instant messengers*) incluindo, no mínimo, *ICQ*, *WhatsApp*, *Google Talk*, *Skype* e IRC, para usuários da rede, individualmente ou em grupo;

1.4.4.7. Deve ter suporte à proteção e identificação de *hosts* possivelmente infectados com *botnets*. A solução ofertada deve permitir ao administrador a possibilidade de apenas registrar e identificar as máquinas possivelmente contaminadas, além de ter a possibilidade de habilitar e analisar todas as conexões que passam por este dispositivo de segurança, bem como ativar tal funcionalidade especificando análise por regra de *firewall*, permitindo assim maior granularidade da gestão e do recurso;

1.4.4.8. Deve ter a capacidade de analisar tráfegos criptografados *HTTPS/SSL*, que deverá ser descriptografado de forma transparente à aplicação;

1.4.4.9. Implementar *DSCP* (*Differentiated Services Code Points*);

1.4.4.10. Possuir mecanismo de forma a possibilitar o funcionamento transparente dos protocolos *FTP*, *SIP*, *RTP*, *RTSP* e *H323*, mesmo quando acessados por máquinas através de conversão de endereços. Este suporte deve funcionar tanto para acessos de dentro para fora quanto de fora para dentro da rede;

1.4.4.11. Implementar controle e gerenciamento de banda para a tecnologia *VoIP* (*Voice Over IP*) sobre diferentes segmentos de rede com inspeção profunda de segurança sobre este serviço.

1.4.4.12. FILTRO DE CONTEÚDO *WEB*

1.4.4.12.1. Possuir filtro de conteúdo integrado ao *NGFW* para classificação de páginas *web* com, no mínimo, 50 (cinquenta) categorias distintas, com mecanismo de atualização e consulta automáticas;

1.4.4.12.2. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais *URLs*, através da integração ao serviço de diretório, *Microsoft Active Directory* e base de dados local;

1.4.4.12.3. Devem ser fornecidas licenças de filtro de conteúdo para cada equipamento e quantidade de usuários ilimitada, provendo atualização automática e em tempo real através da categorização contínua de novos sites da Internet, sem custo adicional, por todo o período de vigência da garantia e do contrato de manutenção e suporte técnico;

1.4.4.12.4. Permitir a customização de página de bloqueio;

1.4.4.12.5. Controle de conteúdo filtrado por categorias de sites com base de dados continuamente atualizada pelo fabricante;

1.4.4.12.6. Deve permitir submissão de novos sites para categorização;

1.4.4.12.7. Permitir a classificação dinâmica de sítios eletrônicos, *URLs* e domínios;

1.4.4.12.8. Permitir a associação de grupos de usuários a diferentes regras de filtragem de sítios eletrônicos, definindo quais categorias deverão ser bloqueadas ou permitidas, para cada grupo de usuários, podendo ainda adicionar ou retirar acesso a domínios específicos da Internet;

1.4.4.12.9. Permitir a definição de quais zonas de segurança serão aplicadas as regras de filtragem de *web*;

1.4.4.12.10. Permitir aplicar a política de filtro de conteúdo baseada em horário do dia e dia da semana.

1.4.4.13. CARACTERÍSTICAS DE AUTENTICAÇÃO

1.4.4.13.1. Prover autenticação de usuários para os serviços *Telnet, FTP, HTTP e HTTPS*, utilizando as bases de dados de usuários e grupos de servidores *Windows* e *Unix*, de forma simultânea;

1.4.4.13.2. Permitir a autenticação dos usuários utilizando servidores *LDAP*, *Active Directory*, *RADIUS*, *Tacacs+*, *Single Sign On* e API;

1.4.4.13.3. Permitir o cadastro manual dos usuários e grupos diretamente no *NGFW* por meio da interface de gerência remota do equipamento;

1.4.4.13.4. Permitir a integração com qualquer autoridade certificadora emissora de certificados *X.509* que siga o padrão de *PKI* (*Private Key Infrastructure*) descrito na *RFC 5280*, e suas atualizações, inclusive verificando os certificados expirados/revogados, emitidos periodicamente pelas autoridades certificadoras, os quais devem ser obtidos automaticamente pelo *NGFW*;

1.4.4.13.5. Permitir o controle de acesso por usuário, para plataformas, no mínimo, *Microsoft Windows* 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 sem a instalação de *softwares* adicionais nas estações de trabalho, sem configuração adicional no *browser* e sem redirecionamento para página de início de sessão no *firewall*, para usuários conectados ao domínio local;

1.4.4.13.6. Para acessos à *internet,* de usuários não conectados ao domínio, é aceito apenas o redirecionamento para página de início de sessão no *firewall*, para iniciar uma autenticação integrada ao domínio local;

1.4.4.13.7. Deve permitir o controle, sem instalação de cliente de *software*, em equipamentos, de qualquer plataforma, que solicitem saída à *internet* para que, antes de iniciar a navegação, redirecione para um portal de autenticação residente no *NGFW*;

1.4.4.13.8. Permitir aos usuários o uso de seu perfil de acesso à *internet*, independentemente do endereço *IP* da máquina que o usuário esteja utilizando;

1.4.4.13.9. Permitir a atribuição de perfil por faixa de endereço IP nos casos em que a autenticação não seja requerida.

1.4.5. **SERVIÇO DE GESTÃO**

1.4.5.1. Permitir a criação de perfis de administração distintos, de forma a possibilitar a definição de diversos administradores para o *NGFW*, cada um responsável por determinadas tarefas da administração;

1.4.5.2. Possuir mecanismo para aplicar remotamente, pela interface gráfica, correções e atualizações para o *NGFW*;

1.4.5.3. Possuir mecanismo para realizar remotamente, através de interface gráfica, cópias de segurança. *backup* e restauração de configurações e sistema operacional;

1.4.5.4. Possuir mecanismo para agendamento realização das cópias de segurança, *backups,* de configuração;

1.4.5.5. Possuir mecanismo para exportar as configurações através de *FTP, HTTPs* ou *SFTP*;

1.4.5.6. A solução deve permitir ao administrador aplicar ajustes rápidos das melhores práticas de segurança no dispositivo com apenas um clique, possibilitando implementar as melhores práticas recomendadas pelo fabricante;

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

1.4.5.8. Permitir a visualização, em forma gráfica, do percentual do uso de *CPU* e quantidade de tráfego de rede em todas as interfaces do *NGFW* em tempo real;

1.4.5.9. Permitir a visualização, em tempo real, dos serviços com maior tráfego e os endereços *IP* mais acessados;

1.4.5.10. Deve suportar, no mínimo, dois tipos de negação de tráfego nas políticas de *firewall*:

1.4.5.10.1. Descarte sem notificação do bloqueio ao usuário, *discard*;

1.4.5.10.2. Descarte com notificação do bloqueio ao usuário, *drop*;

1.4.5.10.3. Descarte com opção de envio de *ICMP Unreachable* para máquina de origem do tráfego;

1.4.5.10.4. *TCP-Reset* para o cliente, *TCP-Reset* para o servidor ou para os dois lados da conexão.

1.4.5.11. Ser capaz de visualizar, de forma direta no *appliance* e em tempo real, as aplicações mais utilizadas, os usuários que mais estão utilizando estes recursos informando sua sessão:

1.4.5.11.1. total de pacotes enviados;

1.4.5.11.2. total de bytes enviados;

1.4.5.11.3. média de utilização em Kbps;

1.4.5.11.4. URLs acessadas; e

1.4.5.11.5. ameaças identificadas.

1.4.5.12. Permitir habilitar auditoria de configurações no equipamento, possibilitando o rastreio das configurações aplicadas no produto;

1.4.5.13. Ser capaz de implementar a funcionalidade de *Zero-Touch*, permitindo que o equipamento se provisione autônoma e automaticamente no sistema de gestão centralizada;

1.4.5.14. Deve suportar modo *Sniffer*, para inspeção via porta espelhada do tráfego de dados da rede;

1.4.5.15. Deve suportar modo misto de trabalho *Sniffer*, *L2* e *L3* em diferentes interfaces físicas;

1.4.5.16. Implementar mecanismo de sincronismo de horário através do protocolo *NTP* (*Network Time Protocol*);

1.4.5.17. Possuir suporte ao protocolo *SNMP* versões 2 e 3;

1.4.5.18. Possuir suporte a log via *syslog;*

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

1.4.6. **SERVIÇO DE RELATÓRIOS**

1.4.6.1. Ser capaz de visualizar, de forma direta no *appliance*, em tempo real, o estado do processamento do produto e *throughput* de dados utilizado pela rede de computadores conectado ao equipamento;

1.4.6.2. Possibilitar a geração de relatório de ameaças, com avaliação e gerenciamento de riscos, e informações detalhadas sobre o ambiente, ajudando a identificar explorações de vulnerabilidades, intrusões e outras ameaças. Deve permitindo o download em formato *PDF*;

1.4.6.3. Ser capaz de visualizar, de forma direta no *appliance,* em tempo real, a largura de banda utilizada por política e por protocolo *TCP/UDP/IPv4* e *IPv6*;

1.4.6.4. Ser capaz de visualizar, de forma direta no *appliance* e em tempo real as conexões estabelecidas, com possibilidade de aplicar filtros na visualização;

1.4.6.5. Possibilitar a geração de, no mínimo, os seguintes tipos de relatório, mostrados em formato *HTML* ou *PDF*:

1.4.6.5.1. máquinas mais acessadas;

1.4.6.5.2. serviços mais utilizados;

1.4.6.5.3. usuários que mais utilizaram serviços;

1.4.6.5.4. *URLs* mais visualizadas;

1.4.6.5.5. categorias *Web* mais acessadas.

1.4.7. **GARANTIA, SUPORTE E LICENCIAMENTO**

1.4.7.1. O licenciamento, garantia e suporte de todos os recursos descritos e os outros, não citados, mas que fazem parte do conjunto do recurso citado, devem contemplar todo período de vigência do contrato de fornecimento do serviço descrito neste Termo de Referência;

1.4.7.2. Deve contemplar a garantia, o suporte técnico e o suporte de manutenção do fabricante, para todo *hardware* e *software* que compõem o serviço, pelo período de vigência do contrato;

1.4.7.3. Deve assegurar a utilização de novas versões de *software* da solução, sempre que essa estiver disponível a qualquer cliente;

1.4.7.4. O suporte do fabricante deve ter um sistema de abertura de chamados para acompanhamento, funcionando regime de 24x7;

1.4.7.5. Para atendimento telefônico, deve operar em língua Portuguesa, no mínimo, em regime 8x5.

1.4.8. **CONFORMIDADES DO SERVIÇO**

1.4.8.1. Deve implementar controle do tráfego para os protocolos *TCP, UDP, ICMP*, e serviços como *FTP, DNS, P2P* entre outros, baseados nos endereços de origem e destino;

1.4.8.2. Implementar recurso de *NAT* (*Network Address Translation*) do tipo *one-to-one*, *one-to-many*, *many-to-many*, *many-to-one*, porta *TCP* de conexão (*NAPT*) e *NAT Traversal* em *VPN IPSec* (*NAT-T*) e *NAT* dentro do túnel *IPSec*;

1.4.8.3. Deve implementar *Network Prefix Translation* (*NPTv6*) ou *NAT66*, prevenindo problemas de roteamento assimétrico;

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

1.4.8.5. Suportar *Equal Cost Multi-Path (ECMP)* no mínimo para roteamento estático e protocolo *OSPF*;

1.4.8.6. Suporte a *Policy-Based Routing* (*PBR*), com a capacidade de roteamento, no mínimo, mas não limitado a, de endereço de origem, endereço de destino, serviço e aplicação;

1.4.8.7. Possuir suporte aos protocolos de roteamento *RIP, OSPF e BGP*. As configurações de *RIP* e *OSPF* devem ser configuradas através da interface gráfica;

1.4.8.8. Reconhecer aplicações, no mínimo, *peer-to-peer*, redes sociais, acesso remoto, *update* de *software*, protocolos de rede, *VoIP*, áudio, vídeo, *proxy*, mensageiros instantâneos, compartilhamento de arquivos e *e-mail*;

1.4.8.9. Controle, inspeção e descriptografia de *SSL/TLS* por política para tráfego de entrada (*Inbound*) ou Saída (*Outbound*) com suporte a, no mínimo, *SSLv2, SSLv3, TLS 1.0, TLS 1.1, TLS 1.2* e *TLS 1.3*;

1.4.8.10. Deve descriptografar pacotes possibilitando a leitura de *payload* dos pacotes para checagem de assinaturas de aplicações conhecidas pelo fabricante.;

1.4.8.11. A solução deverá implementar tecnologia de *SD-WAN* (*Software Defined WAN*);

1.4.8.12. Capacidade de agregar no mínimo 4 (quatro) circuitos *WAN* distintos em um único canal lógico onde seja possível criar controles de caminho automático baseado em políticas, com habilidade de selecionar o melhor caminho, no mínimo, através dos seguintes parâmetros simultâneos: Latência, *Jitter* e Perda de pacotes.;

1.4.8.13. O administrador da solução deverá ter a capacidade de configurar o canal lógico de *SD-WAN* para encaminhar tráfego simultaneamente por todos os *links* pertencentes a esse canal lógico;

1.4.8.14. A comutação do *SD-WAN* deve ocorrer de maneira dinâmica e automática baseada nas políticas aplicadas;

1.4.8.15. A solução de *SD-WAN* deve permitir encaminhamento de tráfego com base em assinaturas de aplicações conhecidas (*DPI*), como *Office 365*, *Facebook* e *Youtube*, bem como aplicações associadas como *Facebook Messenger* e *Office 365 Outlook*;

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

1.4.8.17. Implementar interface *CLI* segura através do protocolo *SSH*;

1.4.8.18. Visando estabelecer efetividade de segurança dos equipamentos e *softwares* e assegurar que a CONTRATADA entregue uma solução já testada e comprovada por um órgão independente de mercado, o fabricante da solução deverá ser avaliado e

certificado pelo *NetSecOPEN*, que poderá ser consultado no sítio eletrônico https://www.netsecopen.org/certifications;

1.4.8.19. Também deverá ser avaliado e citado pelo *Gartner MQ* (*Magic Quadrant for Network Firewalls*), no mínimo, em um dos relatórios publicados dos últimos 24 meses;

1.4.8.20. Caso a CONTRATADA não seja o fabricante/desenvolvedor da solução, deverá fornecer declaração do(s) fabricante(s), em papel timbrado, dos produtos ofertados, declarando que ela possui credenciamento desse para implantação e suporte técnico de seus produtos, no mínimo, na categoria GOLD ou equivalente, demonstrado através de consulta no sítio eletrônico do fabricante;

1.4.8.21. O equipamento deve ser homologado pela ANATEL;

1.4.8.22. A CONTRATADA deve comprovar que possui, em seu quadro de funcionários, no mínimo, 3 (três) profissionais técnicos certificados pelo fabricante, para execução dos serviços descritos neste Termo de Referência.

1.4.9. **DESEMPENHO MÍNIMO DO SERVIÇO**

1.4.9.1. Desempenho em modo *Threat Prevention* (Proteção *Anti-Malware*, *IPS* e Controle de Aplicação habilitados), mínimo de 2 Gbps ou superior;

1.4.9.2. Desempenho em modo de Inspeção (descriptografia e criptografia) de tráfego criptografado (*SSL/TLS*), mínimo de 800 Mbps;

1.4.9.3. Os desempenhos solicitados devem ser comprovados por folha de dados da solução ou outro documento de domínio público do fabricante específico para solução ofertada;

1.4.9.4. Não serão aceitas declarações ou cartas de fabricantes para atendimento deste item;

1.4.9.5. Desempenho *IPS,* no mínimo, de 3 Gbps;

1.4.9.6. Suporte para, no mínimo, 500.000 conexões simultâneas/concorrentes no modo *DPI*;

1.4.9.7. Suporte para, no mínimo, 21.000 novas conexões por segundo;

1.4.9.8. Deve possuir fonte de alimentação com chaveamento automático entre 90V até 240 V AC, em 50 ou 60 Hz;

1.4.9.9. Deve possuir 16 interfaces 1 GE padrão RJ-45;

1.4.9.10. Deve possuir 3 interfaces 10GE SFP+;

1.4.9.11. Deve possuir 1 interface do tipo 1 GE RJ-45 dedicada para gerenciamento do equipamento;

1.4.9.12. Deve possuir 1 interface USB 3.0 com suporte a tecnologias LTE 3G/4G e 5G;

1.4.9.13. O equipamento deverá suportar *VPN Client-to-Site IPsec*, no mínimo, 1000 usuários simultâneos, com aquisição de licença complementar;

1.4.9.14. O equipamento deverá suportar *VPN SSL*, no mínimo, 500 usuários simultâneos, com aquisição de licença complementar;

1.4.9.15. Deve suportar, no mínimo, 2000 túneis de *VPN* tipo *Site-to-Site* padrão *IPSEC* simultâneos;

1.4.9.16. Deve suportar, no mínimo, 2.1 Gbps de desempenho de *VPN IPSEC*;

1.4.9.17. Os desempenhos apontados devem ser comprovados por documento de acesso público no sítio eletrônico do fabricante. A ausência de tais documentos comprobatórios reservará ao SEMAE o direito de solicitar à licitante a aferição da performance dos equipamentos em bancada, e o atendimento de todas as funcionalidades especificadas neste Termo de Referência, em data e horário definidos na sessão licitatória. Caso seja comprovado o não atendimento das especificações mínimas nos testes de bancada, a licitante será considerada inabilitada e todos os custos oriundos do teste de bancada serão por conta da licitante;

1.4.9.18. O fornecimento dos produtos e seus licenciamentos devem ser entregues pela CONTRATADA, mediante o prazo estabelecido neste Termo de Referência;

1.4.9.19. A solução deve consistir em plataforma de proteção de rede baseada em *appliance* com funcionalidades de *Next Generation Firewall* (*NGFW*);

1.4.9.20. Por funcionalidades de *NGFW* entende-se, no mínimo, o que descreve a RFC 9411, disponível para consulta no sítio eletrônico https://datatracker.ietf.org/doc/rfc9411/ (consulta realizada em 08/02/2024);

1.4.9.21. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;

1.4.9.22. Define-se o termo *appliance* como sendo um equipamento dotado de processador, memória, armazenamento interno, interfaces de rede e outros recursos exclusivos para um determinado serviço.

1.4.9.23. Não serão aceitas soluções baseadas em *PC* (*Personal Computer*) de uso geral, e soluções de *appliance* que utilizam *hardware* e *software* de fabricantes diferentes.

2. ESTIMATIVA DO PREÇO

2.1. O valor previamente estimado da contratação é compatível com os valores praticados pelo mercado que foi realizado através de pesquisa com fornecedores, mediante solicitação por *e-mail*, foram 03 cotações, os quais são anexos a este termo. Encontramos uma média mensal para o serviço de R$ 12.010,11, que estão presentes em anexo neste Termo.

3. ADEQUAÇÃO ORÇAMENTÁRIA

3.1. As despesas decorrentes desta contratação estão programadas em dotação orçamentária própria, prevista no orçamento para o exercício de 2024 na classificação abaixo: órgão/elemento de despesa/dotação: - Serviço municipal de água e esgoto; elemento de Despesa: 33904000- Serviços de informática e comunicação e Dotação 12;

3.2. Informamos também, que a despesa em referência por ser classificada despesa contínua está previsto na Lei do PPA – Plano Plurianual e será compatível com a LDO/2024 – Lei de Diretrizes Orçamentária e com a LOA/2024.

4. O PRAZO DE CONTRATAÇÃO

4.1. O prazo deste contrato será de 12 (doze) meses consecutivos e ininterruptos, contados da data estabelecida pela Autorização dos Serviços, podendo ser prorrogado por iguais e sucessivos períodos até o limite de 60 (Sessenta) meses nos termos da lei 14.133/21, podendo ser prorrogados por mais 05 anos conforme o art.108 da lei 14.133/2021, nas condições permitidos pela legislação vigente, desde que as partes se manifestem com antecedência de 90 (noventa) dias do término do prazo do contrato.

5. DOS REQUISITOS DA CONTRATAÇÃO

5.1. INSTALAÇÃO

5.1.1. A contratada deverá instalar o equipamento em parceria com a equipe técnica do Centro de Tecnologia e Informática do SEMAE;

5.1.2. Ficará sob responsabilidade da contratada realizar toda a transferência da configuração hoje existente do equipamento *Sonicwall* NSA 2600 utilizado pela Contratante para os equipamentos objeto desta licitação;

5.2. SUPORTE TÉCNICO REMOTO CONTINUADO

5.2.1. A CONTRATADA deverá prestar, ao longo da vigência do Contrato, serviços de suporte técnico da solução fornecida, os quais devem contribuir para assegurar a continuidade do pleno funcionamento da solução.

5.2.2. Os referidos serviços deverão abranger o atendimento e providências na ocorrência de falhas na solução quando se verifique indisponibilidade, incompatibilidade entre o comportamento observado e as especificações técnicas, configurações inadequadas ou outras circunstâncias, na utilização da mesma, que ponham em risco, com qualquer grau de severidade, a implantação de serviços ou regras de negócios do SEMAE.

5.2.3. Requisitos mínimos dos serviços a serem prestados:

5.2.3.1. Suporte Remoto Especializado com cobertura 24x7x365 dias.

5.2.3.2. Suporte Presencial Especializado com cobertura 24x7x365 para manutenções críticas de indisponibilidade e falta de acesso a recursos de rede dependentes do equipamento.

5.2.3.3. Atendimento Remoto e On-site para resolução de chamados de severidade "Emergencial" e ou "Mau Funcionamento", em português sem limite de chamados, os níveis de severidade estão detalhados em SLA – Acordo de Nível de Serviço.

5.2.3.4. Realizar o acompanhamento das atualizações *Update* e *Upgrade* durante o período de contrato.

5.2.3.5. Suporte Remoto (via *Webex*, *VPN*, *SSH*, *HTTPS*) para realização de manutenção periódica e ajustes do UTM-Firewall.

5.2.3.6. Equipe disponível durante 24 horas x 365 dias para atendimento remoto e/ou on-site com mobilização e deslocamento em até 2 horas após acionamento e orientações do SEMAE. Essa equipe será acionada em casos críticos de parada na rede ocasionados por quaisquer ameaças, devendo a contratada solucionar definitivamente o problema em até 4 horas.

5.2.3.7. Visita técnica programada para a realização de manutenções preventivas e corretivas do sistema, geração de relatórios técnicos e melhorias no ambiente de forma geral. Essa visita deverá ocorrer, no mínimo, 1 (uma) vez a cada 30 dias.

5.2.3.8. A contratada deverá disponibilizar equipamento da mesma marca com características iguais ou superiores ao utilizado pelo SEMAE para contingência em caso de defeito, indisponibilidade, intermitência ou quaisquer outros defeitos que causem impacto direto na disponibilidade dos recursos de rede.

5.2.3.9. A substituição do equipamento defeituoso deverá ocorrer em até 4 horas.

5.2.3.10. Disponibilização das atualizações de versão e patchs de correção dos drivers decomponentes durante o tempo de garantia;

5.2.3.11. Acesso online a documentação e recursos técnicos, base de conhecimento e fóruns de discussão;

5.2.3.12. Número ilimitado de requisições de suporte;

5.2.3.13. Acesso aos recursos de suporte através de telefone e página da Internet.

5.2.4. Os serviços de suporte técnico deverão prevenir o surgimento de problemas nos produtos e auxiliar na solução dos mesmos, através de visita mensal preventiva a ser programada e realizada por técnico da contratada, observando os itens abaixo:

5.2.4.1. Atualização de microcódigos, *firmwares*, *drivers* e *softwares* utilitários;

5.2.4.2. Alteração e adaptação de configurações dentro do escopo contratado;

5.2.4.3. Instalação e desinstalação de módulos e componentes dentro do escopo contratado referente à problemas e/ou falhas ocorridas;

5.2.4.4. Quaisquer outras intervenções na solução de forma a assegurar o bom funcionamento da mesma, de acordo com as necessidades do SEMAE.

5.2.4.5. Deverá ser possível notificar incidentes de falhas à CONTRATADA, via atendimento telefônico, no regime de 24 horas por dia, sete dias por semana, incluindo os feriados, locais, regionais e nacionais. Os chamados telefônicos notificando incidentes deverão ser atendidos em língua portuguesa pela central de atendimento da CONTRATADA;

5.2.4.6. A CONTRATADA deverá disponibilizar relatório com informações sobre o atendimento aos chamados elaborados pelo técnico após as visitas ou atendimentos, detalhando quais procedimentos foram realizados.

5.3. OBRIGAÇÕES DA CONTRATADA

5.3.1. Manter o CONTRATANTE sempre informado de todas as versões e atualizações de software disponibilizadas pelos fabricantes dos softwares contratado, entregando a documentação relativa à nova versão entregue.

5.3.2. Fornecer sempre que solicitado, boletins técnicos e manuais de uso atualizados;

5.3.3. A CONTRATADA deverá fornecer ao SEMAE, proativamente as atualizações, modificações e/ou melhorias introduzidas nos softwares tão logo haja disponibilidade do material.

5.3.4. A CONTRATADA deverá informar proativamente o SEMAE sobre a descoberta de *bugs* nos softwares contratados, durante toda a vigência do contrato.

5.3.5. A CONTRATADA deverá divulgar as descrições destes *bugs e seus* possíveis impactos.

5.3.6. A CONTRATADA deverá apresentar as informações sobre *patches* de correção e o local disponível na Internet onde tais atualizações estarão disponíveis, com as respectivas plataformas suportadas, para todos os softwares contratados.

5.3.7. A CONTRATADA deverá indicar a localização na Internet, para download, das correções lançadas (*patches*).

5.3.8. O SEMAE deverá ter como opção executar ou não as atualizações de softwares disponibilizadas;

5.3.9. Não divulgar dados ou informações relacionadas aos serviços e produtos objeto do presente, mantendo sigilo absoluto em relação a todos os dados acessados ou que venham a ser gerados, no processo de prestação dos serviços;

5.3.10. Serão de inteira responsabilidade e às expensas da CONTRATADA, sem nenhum custo adicional para o SEMAE:

5.3.10.1. Apoio, suporte técnico e logístico eventualmente necessário ao adequado funcionamento da solução;

5.3.10.2. Disponibilização de profissionais qualificados para execução das atividades do projeto e todas as obrigações trabalhistas relacionadas em dia conforme legislação específica;

5.3.10.3. Todos os ônus relativos a transporte, alimentação, e hospedagem de profissionais, transporte e instalação dos equipamentos, ligações telefônicas para suporte técnico durante o processo de implantação da solução, montagem física dos equipamentos que compõem a solução, disponibilização de ferramentas e insumos diversos requeridos durante qualquer das fases de implantação da solução;

5.3.10.4. Configuração lógica dos componentes da solução proposta de forma a viabilizar integralmente os testes a serem realizados como parte da homologação da solução e o adequado funcionamento em ambiente de produção;

5.3.10.5. Atividades de concepção, projeto, planejamento, implementação, suporte técnico, assistência técnica e apoio logístico eventualmente necessário à adequada implantação da solução;

5.3.10.6. Demonstração de todas as características técnicas e funcionalidades previstas na contratação, durante a fase de homologação de funcionalidades da solução;

5.3.10.7. Deverá acionar o suporte técnico diretamente do fabricante dos equipamentos e componentes de sua proposta de preço, caso necessário para a adequada implantação da solução;

5.3.10.8. Especificações técnicas de toda a solução para efeito de instalação elétrica, climatização e pesos.

5.3.11. Correrão por conta, responsabilidade e risco da CONTRATADA as consequências de:

5.3.11.1. Sua negligência, imperícia, imprudência e/ou omissão;

5.3.11.2. Ato ilícito seu, de seus empregados ou de terceiros em tudo que se referir ao objeto desta licitação;

5.3.11.3. Cumprir durante a execução do objeto todas as leis e posturas federais estaduais e municipais pertinentes e vigentes, sendo a única responsável por prejuízos decorrentes de infrações a que houver dado causa;

5.3.11.4. Manter, durante o período de contratação, o atendimento das condições de habilitação exigidas na licitação.

5.3.11.5. Demais disposições contidas no instrumento contratual.

6. DA EXECUÇÃO DO OBJETO

6.1. O prazo deste contrato será de 12 (doze) meses consecutivos e ininterruptos, contados da data estabelecida pela Autorização dos Serviços, podendo ser prorrogado por iguais e sucessivos períodos até o limite de 60 (Sessenta) meses nos termos da lei 14.133/21, podendo ser prorrogados por mais 05 anos conforme o art.108 da lei 14.133/2021, nas condições permitidos pela legislação vigente, desde que as partes se manifestem com antecedência de 90 (noventa) dias do término do prazo do contrato.

6.2. IMPLANTAÇÃO, TESTES, CONDIÇÕES E PRAZO DE ENTREGA.

6.2.1. Os serviços objeto desse termo de referência são compostos de planejamento, instalação, customização, integração, ativação, documentação, suporte técnico, logístico e gerência da implantação dos componentes da solução, além da transferência de conhecimento técnico e atividades de *HandsOn*;

6.2.2. Todas as atividades relacionadas ao planejamento e implantação da solução serão prestadas nas instalações do datacenter do SEMAE;

6.2.3. Por instalação, customização, integração e ativação entendem-se todos os procedimentos relacionados à instalação e configuração, física e lógica, parametrização e testes de quaisquer componentes de hardware e software fornecidos no escopo do Edital, de modo a garantir o pleno funcionamento da solução, inclusive garantindo a operacionalização e integração com os demais componentes de hardware e software atualmente em uso no SEMAE;

6.2.4. A CONTRATADA deverá criar e manter atualizada documentação das atividades, processos, testes, homologação, entrega e conferência, reuniões de trabalho, compromissos e prazos de modo a compor uma documentação final da implantação a ser entregue ao SEMAE no final do processo;

6.2.5. A CONTRATADA caberá demonstrar todas as funcionalidades requeridas para avaliação por parte do SEMAE, as quais deverão ser testadas em todas as variações possíveis, através de testes específicos;

6.2.6. O SEMAE acompanhará todo o procedimento para realização dos testes, não podendo a CONTRATADA realizá-los omitindo quaisquer informações ou métodos utilizados;

6.2.7. Na demonstração das funcionalidades, a CONTRATADA não poderá alegar, em nenhuma hipótese, a utilização de procedimento, ou qualquer técnica protegida por propriedade industrial ou intelectual que impeçam o SEMAE de ter comprovação integral sobre os resultados dos mesmos;

6.2.8. Os testes que deverão ser executados para certificar as funcionalidades implementadas devem abranger, no mínimo:

6.2.8.1. Teste de acesso e navegação dos micros da rede interna;

6.2.8.2. Teste de filtro de navegação em *URL's* bloqueadas;

6.2.8.3. Teste de acesso aos Servidores da *DMZ*, interna e externamente;

6.2.8.4. Teste de criação e acesso de *VPNs*;

6.2.8.5. Teste de intrusão via ferramenta de benchmark;

6.2.8.6. Teste de *Failover* de hardware para validação de alta disponibilidade;

6.2.9. O não atendimento a qualquer desses requisitos ou prazos, por completo ou em parte, sujeitará a CONTRATADA à aplicação das sanções contratuais correspondentes;

6.2.10. Todos os componentes de hardware e software requeridos para atender as funcionalidades exigidas no Edital, mesmo que não estejam especificados e cotados na proposta, serão considerados como parte integrante dos serviços de instalação e deverão ser fornecidos sem ônus adicional.

6.3. MONTAGEM DOS EQUIPAMENTOS E INSTALAÇÃO DA SOLUÇÃO

6.3.1. As atividades de instalação física da solução deverão observar os seguintes aspectos:

6.3.1.1. A montagem completa (Fixação das Componentes no *rack*, Interligação com *Switches*, etc.) da totalidade dos equipamentos entregues, de forma que, ao final, tudo fique organizado e pronto para ser logicamente configurado e utilizado;

6.3.2. Ficará a cargo e às expensas da Contratada:

6.3.2.1. Atividades relacionadas ao cabeamento interno no *rack* do *datacenter* que abrigará a solução, passagem, organização, marcação e rotulação dos componentes envolvidos.

6.3.2.2. Fornecimento de todo o material necessário para essas atividades.

6.3.2.3. Instalação, configuração, ativação e licenciamento de todos os *softwares* que envolve a solução de modo que possibilite a homologação de todas as funcionalidades requeridas no Edital.

6.3.3. A contratante fornecerá o *rack* que abrigará os equipamentos da solução.

6.4. CRITÉRIOS PARA INSTALAÇÃO LÓGICA DA SOLUÇÃO

6.4.1. As seguintes condições deverão ser observadas acerca da execução dos serviços de implantação das funcionalidades técnicas da solução no ambiente:

6.4.1.1. A instalação da solução deverá, preferencialmente, ser efetuada de forma a não afetar o funcionamento dos recursos ou equipamentos atualmente em operação, nem impedir ou interromper a rotina de trabalho de funcionários e colaboradores do SEMAE, devendo ser executada em finais de semana ou horários alternativos ao expediente de atendimento.

6.4.1.2. No caso de necessidade de interrupção dos recursos, equipamentos ou da rotina de trabalho de qualquer setor funcional, em decorrência da instalação da solução, esta deverá estar devidamente planejada e ser acordada com antecedência junto a contratante;

6.4.1.3. As atividades de instalação lógica da solução deverão observar os seguintes aspectos:

6.4.1.3.1. A implantação dos componentes de *software* da solução deverá estar em consonância com a metodologia, parâmetros e funcionalidades indicadas no documento "Plano de Implantação".

6.4.1.4. Deverá ser elaborada juntamente com a equipe técnica do SEMAE, qual a melhor estratégia de *Backup e Restore* dos componentes de software da solução.

6.5. CRONOGRAMA DE EXECUÇÃO

6.6. O quadro abaixo apresenta o cronograma previsto para a implantação da solução;

6.7. Os dias apresentados para execução das atividades devem ser considerados "dias corridos", isto é, dias não úteis como final de semana e feriados devem ser considerados para a execução do projeto e atendimento dos prazos.

Evento	Descrição	Prazo máximo para conclusão
1	Assinatura do contrato	
2	Reunião inicial do projeto, levantamento de informações.	3 dias após a assinatura
3	Entrega do Documento "Plano de Implantação".	5 dias após o evento 2
4	Avaliação pelo SEMAE do Plano de Implantação.	2 dias após o evento 3
5	Emissão do termo de homologação do Plano de Implantação	2 dias após o evento 4
6	Entrega de todos os componentes da solução	30 dias após o evento 1
7	Conferência de todos os componentes entregues da	1 dias após o evento 6
8	Emissão do termo de homologação de recebimento dos equipamentos e software da solução	1 dia após o evento 7
9	Instalação física da solução	3 dias após o evento 8

10	Emissão do termo de homologação da instalação física da solução	1 dia após o evento 9
11	Instalação lógica da solução Período de funcionamento experimental Implantação e testes na solução de backup Eliminação de pendências Período sem falhas	5 dias após o evento 10
12	Emissão do termo de homologação da instalação lógica da solução.	1 dias após o evento 11
13	Acompanhamento operacional do ambiente de redes por parte da CONTRATADA.	5 dias após o evento 12
14	Emissão do termo de homologação da solução implantada	1 dias após o evento 17

6.8. O Prazo de instalação, configuração e entrega do serviço é de até 60dias, podendo ser prorrogado a data com o vencedor do certame.

ACORDO DE NÍVEL DE SERVIÇOS – SLA

6.8.1. O objetivo deste Acordo de Nível de Serviço (SLA) é definir as responsabilidades e dependências entre a CONTRATADA e o CONTRATANTE para os serviços e produtos contratados.

6.8.2. Os acordos operacionais previstos neste documento não devem ter precedência nem limitar as respectivas obrigações e responsabilidades já descritas no contrato feito entre o SEMAE e a CONTRATADA.

6.8.3. Este SLA descreve como o SEMAE e a CONTRATADA irão tratar seu relacionamento, para assegurar que os serviços serão corretamente entregues.

6.8.4. Define os compromissos requeridos entre a CONTRATADA - como provedora de serviços e tecnologias e o SEMAE, para a entrega dos serviços contratados.

6.8.5. **SEVERIDADE**

6.8.5.1. Os níveis abaixo devem ser observados para classificação de severidade na abertura de chamados ao Suporte Técnico, devendo ser registrados no momento do atendimento.

Severidade	**Descrição**	**Tempo máximo para início do atendimento**
Emergencial	Falha no sistema, fora de operação, interrompido	1 hora
Mau Funcionamento	Falha intermitente em serviços suportados que torne o ambiente lento ou em pequenos grupos a operação está afetada, mas sem interrupção. Ajustes de configuração para liberação de acesso a sites restritos ou downloads de arquivos cuja extensões estejam bloqueadas.	2 horas
Atividade Remota Programada	Realização de manutenção preventiva, atualizações e atividades agendadas.	12 horas

6.8.5.2. Os prazos acima relacionados serão computados a partir do momento de abertura do chamado pelo funcionário do SEMAE a central de suporte da CONTRATADA.

6.8.6. **CRITÉRIOS PARA ABERTURA DE CHAMADOS TÉCNICOS**

6.8.6.1. A CONTRATADA deverá prestar o serviço de suporte nas modalidades *Web* ou telefônica, em idioma português do Brasil.

6.8.6.2. A CONTRATADA deverá manter o serviço de suporte técnico disponível para abertura e acompanhamento de chamados em tempo integral 24x7 (vinte e quatro horas por dia, sete dias por semana, todos os dias do ano, inclusive sábados, domingos e feriados).

6.8.6.3. A CONTRATADA deverá garantir que o SEMAE efetue um número ilimitado de chamados de suporte durante a vigência do Contrato para suprir suas necessidades de utilização, sem ônus adicional.

6.8.6.4. A CONTRATADA deverá fornecer um número de telefone que possibilite ligações para sua o suporte técnico, para fins de abertura e acompanhamento de chamados. A

ONTRATADA deverá fornecer acesso a pelo menos 3 (três) pessoas autorizadas para abertura e acompanhamento de chamados de suporte.

6.8.6.5. Na abertura de cada chamado técnico deverá ser emitido um registro contendo informações detalhadas do chamado.

6.8.6.6. Uma vez feito o contato por este número de telefone, a CONTRATADA terá os prazos estabelecidos nos termos deste Acordo de Nível de Serviços para dar uma solução à ocorrência, conforme seu grau de severidade.

7. DOS CRITÉRIOS DA MEDIÇÃO E PAGAMENTO

7.1. PAGAMENTO

7.1.1. O pagamento da nota fiscal, tão logo seja aceita pelos gestores e/ou Diretor Geral, será efetuado após 20 dias corridos da liberação do aceite do laudo, fatura ou nota fiscal, através de crédito em conta corrente, em nome da contratada, ou primeiro dia útil subsequente a esta, quando for feriado ou ponto facultativo do Poder Executivo.

7.1.2. A nota fiscal deve ser encaminhada ao departamento/setor requisitante indicadas no campo NOTAS da Autorização de Fornecimento que após o seu aceite, encaminhará para o Departamento Financeiro para as devidas providências.

7.1.3. Quando da emissão da Nota Fiscal de bens e de serviços, empresa deverá destacar o imposto de renda a ser retido na fonte, de acordo com INF RFB 1.235/2012 e suas alterações através da INF RFB 2.145/2023 e atendimento ao Decreto Municipal 22.122/2023.

7.1.4. Quem fará a retenção será a Autarquia e não a empresa.

7.1.5. Todas as notas fiscais, faturas ou quaisquer outros documentos de cobrança deverão ser emitidos com o destaque do Imposto de Renda a ser retido, além das demais retenções (Contribuição Previdenciária, ISSQN, etc.), quando for o caso, sendo que não serão efetuadas as retenções de CSLL, PIS/PASEP e COFINS.

7.1.6. Nos termos do artigo 4º do Decreto Municipal nº 22.122/2023, é condição para o recebimento e aceitação das notas fiscais, faturas e quaisquer outros documentos de cobrança referente a fornecimento de bens ou prestação de serviços, que o documento tenha destacado o valor do Imposto de Renda (IR) Retido na Fonte e que este seja deduzido da fatura ou eventual boleto para pagamento.

7.1.7. A nova sistemática do Imposto de Renda (IR) Retido na Fonte não trará qualquer impacto econômico-financeiro, uma vez que o valor do imposto retido será considerado como antecipação do valor que for devido a título de Imposto de Renda, pela pessoa jurídica fornecedora de bens ou prestadora de serviços.

7.1.8. As empresas prestadoras de serviços domiciliadas em fora do município de Mogi das Cruzes, cujas operações impliquem em retenção do ISSQN em seu município de origem, deverão realizar e comprovar inscrição no Cadastro de Prestadores de Serviços de Outros Municípios – CPOM, antes da emissão do documento fiscal, para que o imposto não seja retido em duplicidade.

7.1.9. As instruções para cadastramento estão disponíveis no site: http://www.mogidascruzes.sp.gov.br/servico/impostos-e-taxas/iss-cadastro-de-prestadores-de-servicos-de-outros-municipios-cpom/.

7.1.10. Ficam dispensadas do cadastramento no CPOM as pessoas jurídicas estabelecidas fora do município de Mogi das Cruzes que prestarem os serviços dos itens: 4.03, 4.17, 5.02, 5.03, 6.05, 8.01, 8.02 e 9.01 da Lei Complementar Municipal 134/2017.

7.1.11. A não apresentação dessas comprovações assegura a CONTRATADA o direito de suspender o pagamento respectivo e/ou os pagamentos seguintes, até a comprovação da regularização;

7.2. REAJUSTE DE PREÇOS

7.2.1. Para o reajustamento dos preços unitários contratados, deverá ser observada a legislação vigente, sendo a fórmula de cálculo do índice a seguinte:

7.2.2. $R = P_0 . \left[\left(\frac{IPC}{IPC_0} \right) - 1 \right]$

7.2.3. Onde:

7.2.3.1. **R** = parcela de reajuste;

7.2.3.2. **P_0** = preço inicial do contrato no mês de referência dos preços ou preço do contrato no mês de aplicação do último reajuste;

7.2.3.3. **IPC/IPC_0** = variação do IPC FIPE - Índice de Preço ao Consumidor, ocorrida entre o mês de referência de preços, ou o mês do último reajuste aplicado, e o mês de aplicação do reajuste.

Serviço Municipal de Águas e Esgotos
Rua Otto Unger, 450 - Centro
CEP 08780-908 - Mogi das Cruzes – SP
(11) 4798-5105

8. FORMA E CRITÉRIOS DA SELEÇÃO DO FORNECEDOR

8.1. SELEÇÃO DO FORNECEDOR

8.2. A vencedora da licitação deverá comprovar que possui em seu quadro de funcionários, pelo menos (2) dois Profissionais Técnicos Certificados pelo fabricante, na execução dos serviços de instalação, manutenção e treinamento.

8.3. A proponente vencedora caso não seja o fabricante/desenvolvedor da solução, deverá fornecer declaração do(s) fabricante(s), em papel timbrado com firma reconhecida, dos produtos ofertados, declarando que a proponente possui credenciamento do mesmo para a implantação e suporte técnico de seus produtos, pelo menos na categoria GOLD, com tal comprovação sendo emitida pelo fabricante em: https://www.sonicwall.com/pt-br/partners/authorized-distributors

Fabiana Mota de Oliveira

Diretora Administrativa