SERVIÇO MUNICIPAL DE ÁGUA E ESGOTO – SEMAE
Autarquia Municipal - Lei Municipal n.º 1.657 de 30 de abril de 1969
Rua XV de Novembro, 2.200 – Piracicaba/SP – CEP 13.417-100
Fone: (19) 3403-9611 - ramal 9686 - Fax: (19) 3426-9234
www.semaepiracicaba.sp.gov.br

97

DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO

TERMO DE REFERÊNCIA

***Objeto*: Contratação de empresa especializada em comunicação de dados por meio de rede IP para prestação de serviços de infraestrutura para tráfego e armazenamento de backup remoto, com fornecimento de conexão à internet através de acesso dedicado com proteção anti-DDoS nativa e espaço para armazenamento em "nuvem", por 36 (trinta e seis) meses em conformidade com o especificado:**

1. DOS SERVIÇOS

1.1 Prestação de serviços de infraestrutura para tráfego e armazenamento de backup remoto, com fornecimento de conexão à internet através de acesso dedicado com proteção anti-DDoS nativa e espaço para armazenamento em "nuvem" de acordo com as especificações técnicas apresentadas neste Anexo.

2. ABRANGÊNCIA DO SERVIÇO A SER CONTRATADO

2.1 O acesso à internet contratado será utilizado pelo SEMAE como uma infraestrutura híbrida para prover o acesso à sites e e-mails hospedados localmente através da Internet, navegação de usuários e para trafegar dados para armazenamento de backup remoto.

2.2 A contratada não poderá bloquear, limitar ou filtrar de forma alguma o tráfego de entrada ou de saída do link, exceto por solicitação expressa do SEMAE.

2.3 O proponente deve ser o proprietário do link de conexão à internet diretamente ao cliente desde backbone.

2.4 O proponente deverá apresentar, no momento da assinatura do contrato, projeto com autorização da CPFL (Companhia Paulista de Força e Luz), para utilização dos postes do município de Piracicaba no trajeto até o SEMAE.

3. PRAZO PARA IMPLANTAÇÃO DOS SERVIÇOS

3.1 A contratada terá o prazo máximo de 45 (quarenta e cinco) dias, contados da data de assinatura do contrato, para realizar integralmente toda a instalação, configuração e ativação dos serviços, estando a rede totalmente operacional ao término deste prazo.

4. REQUISITOS ESPECÍFICOS DO SERVIÇO – ACESSO À INTERNET

4.1 O circuito deverá ser provido por acesso digital dedicado por meio não compartilhado por outra porta, para conexão a um roteador de borda do backbone da licitante, com taxa mínima efetiva de 100 mbps (cem megabits por segundo), balanceável conforme demanda, dividido em, no mínimo, 2 (duas) interfaces físicas.

4.2 O circuito de acesso deverá absorver 100% (cem por cento) do tráfego da internet referente à velocidade contratada, garantindo o não descarte de pacotes para a faixa coberta pela capacidade contratada para essa porta.

4.3 O meio físico de chegada - "última milha" - ao SEMAE deverá ser através de cabo ótico, não sendo permitido o uso de par metálico para este fim.
4.4 O equipamento de conversão ótico-elétrico também deverá ser fornecido pela contratada e será instalado nas dependências do SEMAE.
4.5 A contratada deverá fornecer todos os ETRs (Equipamentos Terminais de Rede) e se responsabilizar por sua manutenção a fim de garantir os níveis de serviço contratados, devendo seu custo estar contemplado nos preços apresentados em sua proposta.
4.6 Todos os ETRs deverão atender as configurações especificadas no item 8 deste Anexo.
4.7 A contratada será responsável pelos serviços de configuração e gerenciamento até a porta LAN de seus ETRs, de forma a garantir o nível dos serviços contratados.
4.8 Deverá ser disponibilizada duas faixas de endereços IPv4 roteáveis na internet.
4.9 A faixa IP deverá possuir, no mínimo, 8 (oito) endereços IPv4 roteáveis na internet.
4.10 Deverá haver possibilidade do DNS (Domain Name System - Sistema de Nomes de Domínios) reverso na faixa de endereçamento IPv4 serem resolvidos por servidores indicados pela Divisão de TI do SEMAE.
4.11 Todos os endereços IPv4 fornecidos deverão pertencer a um AS - Autonomous System (Sistema Autônomo) da própria empresa, não sendo aceitos endereços pertencentes a terceiros.

5. *REQUISITOS ESPECÍFICOS DO SERVIÇO – ARMAZENAMENTO DE BACKUP REMOTO*

5.1 A licitante deverá informar onde o serviço será prestado, ou seja, o endereço dos servidores de backup, obrigatoriamente localizado em território nacional;
5.2 O backup deve ser estabelecido em servidor com processadores, memórias e discos de alta capacidade, garantindo o desempenho necessário;
5.3 A licitante deverá disponibilizar alternativa de contingência para soluções em caso de falhas no sistema, inclusive mantendo redundância em infraestrutura;
5.4 O serviço deverá estar disponível em tempo integral, 24h por dia, 7 dias por semana;
5.5 O ambiente de tráfego das informações deve permanecer protegido por firewall;
5.6 A licitante licenciará um software de gestão de arquivos no sistema, que realize a tarefa de backup online, de forma a atender às condições impostas;
5.7 A solução de backup deve gerenciar ao mínimo 06 TB (seis terabytes) de dados, de forma permanente e sem restrições, mediante sistema que garanta o sigilo dos dados armazenados e que permita a substituição dos arquivos antigos por suas alterações;
5.8 O sistema deve conter um sistema de buscas que realize a indexação pelo conteúdo do arquivo armazenado;
5.9 Os dados armazenados no sistema de armazenamento devem ser cifrados com chave simétrica pela solução de armazenamento;
5.10 O sistema informará periodicamente o espaço disponível e emitirá alertas quando o limite da capacidade total estiver próximo de ser atingido.

93

6. *REQUISITOS ESPECÍFICOS DO SERVIÇO – ANTI-DDoS*

6.1 Características Técnicas de mitigação Anti-DDoS

6.1.1 A solução deve proteger a infraestrutura de Data Center como um todo, incluindo Firewall e IPS de borda, balanceadores e servidores HTTP e DNS (no caso, proteger suas tabelas de sessão e sockets de um ataque DDoS de longa duração e baixa banda);

6.1.2 Deverá operar sem tabela de sessão, do tipo "*stateless*";

6.1.3 A proponente deve mitigar ataques por 3 horas, caso o ataque ultrapasse o SLA de mitigação contratado;

6.1.4 O sistema de proteção em deverá estar implementado direto no backbone provedor do link de internet;

6.1.5 O proponente deve verificar 100% do tráfego de entrada do link para o datacenter, e no caso de um ataque menor que o tamanho do link, este equipamento deve mitigar conforme especificado neste caderno técnico na sessão de Contramedidas;

6.1.6 Caso o volume de tráfego do ataque ultrapasse as capacidades de mitigação especificadas ou sature as conexões do AS, devem ser tomadas contramedidas tais como aquelas que permitam o bloqueio seletivo por blocos de IP de origem no AS pelo qual o ataque esteja ocorrendo, utilizando técnicas como Remote Triggered Black Hole;

6.1.7 A solução de detecção e mitigação devem possuir serviço de atualização de assinaturas de ataques;

6.1.8 A proponente deve disponibilizar um Centro Operacional de Segurança (ou SOC - Security Operations Center) no Brasil, com equipe especializada em monitoramento, detecção e mitigação de ataques, com opção de atendimento através de telefone 0800, correio eletrônico, em idioma português brasileiro, durante as 24 (vinte e quatro) horas do dia, nos 7 (sete) dias da semana, no período de vigência contratual;

6.1.9 A mitigação de ataques deve ser baseada em arquitetura na qual há o desvio de tráfego suspeito comandado pelo equipamento de monitoramento, por meio de alterações do plano de roteamento;

6.1.10 Em momentos de ataques DOS e DDOS, todo trafego limpo deve ser reinjetado na infraestrutura da contratante através de tuneis GRE (Generic Routing Encapsulation), configurado entre a plataforma de DOS e DDOS da contratada e o CPE do contratante;

6.1.11 Para a mitigação dos ataques não será permitido o encaminhamento do tráfego para limpeza fora do território brasileiro;

6.1.12 As funcionalidades de monitoramento, detecção e mitigação de ataques devem ser mantidas em operação ininterrupta durante as 24 (vinte e quatro) horas do dia, nos 7 (sete) dias da semana, no período de vigência contratual;

6.1.13 Em nenhum caso será aceito bloqueio de ataques de DOS e DDOS por ACLs em roteadores de bordas da contratada;

6.1.14 A contratada deve realizar a detecção de ataques em até 15 (quinze) minutos;

6.1.15 O sistema de mitigação em linha deve poder se comunicar com o centro de limpeza do proponente e de forma manual e

automática, solicitar a mitigação na nuvem, conforme programado pelo usuário;

6.1.16 O sistema de mitigação em linha deve mostrar na tela de dashboard, o montante que está sendo mitigado na nuvem em tempo real (banda e pacotes por segundo);

6.1.17 O operador pode iniciar a mitigação na nuvem, a partir do equipamento em linha, e finalizá-la, conforme necessário;

6.1.18 O equipamento em linha, deve possuir thresholds, onde o operador poderá escolher qual o percentual do ataque, em banda ou pacotes por segundo, o equipamento inicia mitigação automática na nuvem;

6.1.19 O equipamento em linha, deve possuir por obrigatoriedade, a função de selecionar mitigação na nuvem, apenas aos endereços IP's que estiverem sendo atacados, e não o tráfego como um todo;

6.1.20 O sistema em linha deve se comunicar com o sistema na nuvem, de forma automática a cada minuto, através da interface de gerência para prevenir que eventual entupimento do link cesse sua comunicação;

6.1.21 O operador na nuvem, poderá iniciar a mitigação na nuvem, sem que o equipamento em linha acuse necessidade.

6.2 Características de Contramedidas

6.2.1 Deve possuir as seguintes contramedidas no sistema:

6.2.1.1 Invalid Packets - drops invalid IP/TCP/UDP/ICMP packets
6.2.1.2 Dynamic Blacklist (setada por outras contramedidas)
6.2.1.3 IP Address Filter Lists
6.2.1.4 Black / White Lists
6.2.1.5 Inline Filter
6.2.1.6 Black / White Filter Lists
6.2.1.7 Blacklist Fingerprints
6.2.1.8 IP Location Filter Lists
6.2.1.9 Zombie Detection (dinamicamente bloqueando hosts, não permanentemente)
6.2.1.10 Per Connection Flood Limiting
6.2.1.11 TCP SYN Authentication (incluir autenticação HTTP, via 302, redirect, javascript)
6.2.1.12 DNS Authentication (através de requisição ao cliente via TCP)
6.2.1.13 TCP Connection Limiting
6.2.1.14 TCP Connection Reset
6.2.1.15 Payload Regular Expression Filtering
6.2.1.16 Source /24 Baseline Enforcement
6.2.1.17 Protocol Baseline Enforcement
6.2.1.18 DNS Malformed
6.2.1.19 SIP Malformed
6.2.1.20 Shaping
6.2.1.21 IP Location Policing

6.2.2 Invalid packets (pacotes inválidos) deve checar por obrigatoriedade:

6.2.2.1 Malformed IP Header
6.2.2.2 Incomplete Fragment
6.2.2.3 Bad IP Checksum

6.2.2.4 Duplicate Fragment
6.2.2.5 Fragment Too Long
6.2.2.6 Short Packet
6.2.2.7 Short TCP Packet
6.2.2.8 Short UDP Packet
6.2.2.9 Short ICMP Packet
6.2.2.10 Bad TCP / UDP Checksum
6.2.2.11 Invalid TCP Flags
6.2.2.12 Invalid ACK Number

6.2.3 Mitigações obrigatórias em IPv6:
6.2.3.1 Invalid Packets
6.2.3.2 IPv6 Address Filter Lists
6.2.3.3 Black / White Lists
6.2.3.4 Zombie Detection
6.2.3.5 TCP SYN Authentication
6.2.3.6 Payload Regular Expression

6.2.4 O sistema em linha e na nuvem, devem possuir suporte a CDN, impedindo que o IP da CDN seja bloqueado em alguma contramedida;

6.2.5 O sistema em linha e na nuvem devem proteger contra as principais ferramentas e ataques abaixo:
6.2.5.1 Ping Attack, Smurf Attack, reflection attacks, UDP flood, Stream, dc++, blackenergy;
6.2.5.2 Teardrop, Targa3, Jolt2, Nestea;
6.2.5.3 Loic, Hoic, Ref Ref, Slow-Loris, R.U.D.Y;

6.2.6 O sistema deve possuir capacidade de bloquear tráfego através de expressões FCAP;

6.2.7 O sistema deve possuir capacidade de bloquear tráfego através de pay-load regex;

6.2.8 O sistema em linha deve possuir na dashboard (web UI), tela de captura de pacotes, de forma simples e sem onerar a capacidade de processamento de mitigação;

6.2.9 O sistema na nuvem deve possuir a capacidade de criar limites de tráfego, baseado em:
6.2.9.1 Zombie Detection
6.2.9.2 DNS Rate Limiting
6.2.9.3 HTTP Rate Limiting
6.2.9.4 SIP Request Limiting

6.2.10 O sistema inline, deve possuir capacidade de criar limites de http request por segundo, dns request por segundo, dns NX resposta por segundo, Request SIP por segundo;

6.2.11 O sistema inline deve possuir capacidade de criar regras de traffic shape (qos) para servidores e ou IP's internos;

6.2.12 O sistema inline e o sistema na nuvem, devem possuir a capacidade de bloquear, também baseado em:
6.2.12.1 HTTP Malformed
6.2.12.2 HTTP Rate Limiting
6.2.12.3 HTTP/URL Regex
6.2.12.4 SIP Malformed
6.2.12.5 SIP Request Limiting
6.2.12.6 DNS Authentication
6.2.12.7 DNS Malformed
6.2.12.8 DNS Rate Limiting

6.2.12.9 DNS Regex
6.2.12.10 Payload Regex
6.2.13 O sistema na nuvem, deve possuir capacidade de proteger contra ataques DDoS amplificados, como:
6.2.13.1 DNS Reflection
6.2.13.2 NTP Reflection
6.2.13.3 SIP Reflection
6.2.13.4 SSDP Reflection
6.2.13.5 DNS Dicionário
6.2.14 O sistema deve proteger os seguintes ataques em SSL:
6.2.14.1 Malformed SSL Attacks
6.2.14.2 SSL Resource Exhaustion attacks
6.2.14.3 TCP connection exhaustion on TLS ports
6.2.15 O sistema deve proteger as seguintes portas SSL/TLS conforme especificado acima:
6.2.15.1 443 HTTP over TLS (HTTPS)
6.2.15.2 465 SMTP over TLS (legacy SMTPS)
6.2.15.3 Reassigned by IANA as URL Rendezvous Directory for SSM
6.2.15.4 563 NNTP over TLS (NNTPS)
6.2.15.5 587 SMTP mail submission (may be TLS)
6.2.15.6 636 LDAP over TLS (LDAPS)
6.2.15.7 989 TTP over TLS (FTPS)
6.2.15.8 992 TELNET over TLS
6.2.15.9 993 IMAP4 over TLS (IMAP4S)
6.2.15.10 994 IRC over TLS
6.2.15.11 995 POP3 over TLS (POP3S)
6.2.15.12 5061 SIP over TLS.

7. REQUISITOS ESPECÍFICOS DO SERVIÇO - SLA - SERVICE LEVEL AGREEMENT (ACORDO DE NÍVEL DE SERVIÇO)

7.1. O acesso à Internet deverá estar disponível 24x7 (vinte e quatro horas por dia, sete dias por semana).

7.2. Caso seja necessária interrupção no serviço, a contratada deverá comunicar a Divisão de TI do SEMAE com antecedência mínima de 2 (dois) dias úteis.

7.3. Não serão computadas no cálculo de disponibilidade mensal até 3 (três) interrupções anuais do serviço, desde que avisadas conforme item anterior, e utilizadas como janela de manutenção preventiva e corretiva.

7.4. O prazo máximo para solução de quaisquer problemas de hardware, inoperância de acesso decorrente de defeito físico do próprio circuito ou configuração lógica dos ETRs será de 4 (quatro) horas; em casos de danos causados comprovadamente por terceiros, intempéries, desastres e/ou situações de calamidade pública (condições anormais) este prazo será reconsiderado. No entanto, a contratada deverá manter esquemas de contingência (redirecionamento de circuitos, pares de fibras reservas, balanceamento) para que o serviço seja restabelecido dentro do prazo informado em condições normais. O prazo de 4 (quatro) horas foi determinado levando em consideração a criticidade dos serviços envolvidos, que dependem da transmissão de dados através deste link.

7.5. A contratada deverá apresentar como requisito contratual obrigatório, um índice de disponibilidade média mensal de 99,4% (noventa e nove vírgula quatro por cento), da rede de acesso contratada e, no mínimo, 99,8% (noventa e nove vírgula oito por cento) para seu backbone.

7.6. Eventuais indisponibilidades (exceto o limite estabelecido no item 5.3) serão computadas em horas e minutos e serão enviadas à Gestão de Contratos do SEMAE para apuração e eventual desconto proporcional no pagamento mensal.

8. REQUISITOS ESPECÍFICOS DO SERVIÇO – GERÊNCIA DA REDE

8.1. A contratada deverá prover um serviço de gerencia proativa de rede que atue não só em seu backbone, mas também nos acessos contratados pelo SEMAE e em todas as portas WAN dos ETRs instalados.

8.2. A Divisão de TI do SEMAE manterá monitoração sobre os ETRs da contratada, devendo esta prover acesso SNMP somente leitura e todo suporte necessário para tal.

8.3. A gerência de rede deverá disponibilizar contato alternativo a Central de Atendimento para relato de problemas e abertura de chamados, que atue 24 (vinte e quatro) horas por dia.

8.4. Será função da gerência de rede da contratada realizar ações proativas que permitam garantir os níveis de serviço contratados ao retardo, disponibilidade e desempenho da rede contratada.

8.5. Na ocorrência de qualquer falha nos acessos ou nos ETRs instalados no SEMAE a gerência de rede da contratada deverá iniciar o processo de recuperação de falhas fazendo o registro da ocorrência e o posterior acompanhamento de sua solução.

8.6. A Divisão de TI do SEMAE deverá ser contatada pela gerência de rede da contratada por telefone e através de meio eletrônico (e-mail) para informar a indisponibilidade ou falha identificada, para que seja possível verificar prontamente a possibilidade da causa da falha ter ocorrido por falta de energia elétrica ou por outro motivo de responsabilidade do próprio SEMAE.

8.7. A contratada deverá disponibilizar a Divisão de TI do SEMAE acesso a ferramentas que permitam emitir relatórios, gráficos e afins para demonstrar a qualidade dos serviços e permitir análise das configurações e do desempenho dos ETRs instalados.

8.8. Os relatórios deverão conter, no mínimo, as seguintes informações:

8.9. Identificação do ponto de acesso com respectivo número de linha e velocidade disponível.

8.10. Total de horas do período faturado, volume de tráfego (29 dias * 24 horas = 696 horas, onde trafegaram XXX gb de dados, por exemplo).

8.11. Taxa média de ocupação do link (throughput).

8.12. Visualização de gráfico detalhando a utilização da banda.

9. REQUISITOS ESPECÍFICOS DO SERVIÇO – CENTRAL DE ATENDIMENTO

9.1. A contratada deverá dispor de um número 0800 nacional não tarifado e um endereço eletrônico (website e e-mail) para que os técnicos da Divisão de TI do SEMAE possam encaminhar as solicitações de reparo e ou reconfiguração dos ETRs.

9.2. O serviço de registro de chamadas deverá estar disponível 24x7 (vinte e quatro horas por dia, sete dias por semana).

9.3. A Central de Atendimento deverá dar suporte a chamados referentes a rede física (instalação, recuperação, alteração e remoção), configuração de roteadores, roteamentos, endereçamentos IP, SNMP e segurança (incidentes de segurança, senhas, entre outros), considerando-se todos os serviços contratados, de maneira a assegurar a integridade dos meios de comunicação ponto-a-ponto.

10. CONFIGURAÇÕES BÁSICAS DOS EQUIPAMENTOS

10.1. Os serviços de comunicação de dados a serem fornecidos deverão prover todos os ETRs (Equipamentos Terminais de Rede) a serem instalados.

10.2. Todos os roteadores fornecidos deverão ser de uma mesma marca e devem possuir:

10.2.1 A quantidade mínima de memória necessária para atender de forma plena todas as funcionalidades exigidas neste Anexo, conforme recomendações do fabricante.

10.2.2 Conectividade e interligação ao ambiente do Data Center do SEMAE, devendo ser fornecido todo o material e mão de obra necessários através da contratada.

10.2.3 Suporte a QOS.

11. ATRIBUIÇÕES E RESPONSABILIDADES DAS PARTES

11.1. Em caso de falha ou inoperância de qualquer componente instalado, é obrigação da contratada abrir um chamado técnico imediatamente após a constatação do problema, e informar a Divisão de TI do SEMAE sobre a anomalia.

11.2. A Divisão de TI do SEMAE deverá tomar as providências necessárias de modo a permitir ao técnico da contratada acessar os equipamentos onde os serviços serão efetuados, assim como se obriga a disponibilizar pessoal devidamente habilitado e ciente das medidas a serem adotadas para a perfeita integração do produto a instalação, com conhecimento do serviço ou que já tenha recebido treinamento anterior fornecido pela contratada.

11.3. A contratada deverá nomear, no início da vigência do contrato, um gestor e este será o responsável pelo correto encaminhamento de solicitações e ocorrências, caso a central de serviços não opere satisfatoriamente, ainda que por um curto intervalo de tempo.

11.4. A Divisão de TI do SEMAE deverá nomear uma ou mais pessoas autorizadas a solicitar alterações e atualizações a contratada.

11.5. A contratada compromete-se a designar profissionais plenamente capacitados para prestar suporte técnico ao SEMAE.

11.6. O ingresso de pessoas não pertencentes ao corpo técnico da contratada nas dependências do SEMAE deverá ser comunicado via e-mail ou fax, com antecedência mínima de 48 (quarenta e oito) horas.

11.7. A cada visita técnica realizada nas dependências do SEMAE a contratada deverá emitir um relatório de execução das atividades, relacionando os serviços executados e lista de equipamentos que eventualmente sejam instalados, substituídos ou retirados.

11.8. O SEMAE será responsável somente pelos equipamentos que estiverem instalados em suas dependências.

11.9. Em caso de falha em qualquer hardware que compõe a solução, a contratada terá o prazo máximo de 4 (quatro) horas para substituição do equipamento avariado.

11.10. O prazo de instalação para disponibilidade dos serviços terá início a partir da assinatura do contrato.

11.11. O faturamento mensal será iniciado a partir do aceite da instalação e disponibilidade do serviço contratado como um todo.

12. ENDEREÇO DE INSTALAÇÃO DOS EQUIPAMENTOS NO AMBIENTE DA CONTRATANTE PARA ESTABELECIMENTO DO LINK

12.1 Os equipamentos (ETR's) a serem utilizados para estabelecimento do link deverão ser instalados no Data Center do SEMAE, localizado na Rua XV de Novembro, 2.200, 1° andar - Bairro Alto, Piracicaba/SP, devidamente instalados conforme versa o item 10.2.2.

José Odivaldo Chitolina Junior
Divisão de Tecnologia da Informação