

PREGÃO PRESENCIAL 19/2018

ANEXO I - TERMO DE REFERÊNCIA

Os custos estimados foram calculados com base nas cotações prévias de mercado e nos valores efetivamente pagos atualmente pela Prefeitura Municipal, conforme segue:

Item	Descrição dos Serviços	R\$ Global Mensal
01	Prestação de serviços de telefonia, internet e segurança digital;	37.431,04

Das Especificações:

1 - VOZ

A) TRONCOS DIGITAIS E1

- Fornecer troncos digitais E1 com 30 canais ou mais cada link, e faixas DDR nas quantidades estabelecidas no Anexo I.
- Interface tipo G.703.
- Sinalização de Linha tipo R2D.
- Sinalização de Registro tipo MFC 5C.
- Ativar e desativar troncos conforme necessidade da CONTRATANTE e segundo o limite estabelecido na lei nº 8.666/93.
- Prazo de instalação: de 10 a 20 dias no perímetro urbano.
- Prazo máximo contratual de transferência de endereço de instalação: até 15(quinze) dias no perímetro urbano.
- Em locais afastados ou zona rural a instalação será efetivada mediante aprovação de orçamento pela contratante.
- Disponibilidade mensal (SLA - Service Level Agreement) de 99% ao mês.
- Início de atendimento em caso de defeito em até 4 horas.
- Meio de atendimento em par-metálico, fibra-óptica.
- Em casos onde for constatada inviabilidade de instalação a CONTRATADA deverá encaminhar as condições de atendimento (custo, prazo e meio) para análise da CONTRATANTE e será objeto de aditivo contratual.
- Central de Atendimento 24h por dia, 365 dias por ano através de um número 0800.
- A CONTRATADA deverá manter a mesma numeração atualmente utilizada (números de telefone) conforme critérios da Portabilidade regulamentada pela ANATEL, para os números existentes, além de outros que tiverem sua inclusão neste certame.
- O quantitativo de linhas relacionadas no Anexo I é estimado, podendo sofrer alterações até a data da assinatura do contrato. A CONTRATANTE deverá cobrar a quantidade efetivamente instalada.
- A CONTRATADA deverá atender em um prazo de 30 dias corridos solicitações para ampliação de ramal DDR sempre em múltiplos de 10.

B) SERVIÇO ESPECIAL - REDE INTELIGENTE 0800

- Características mínimas:

- Fornecer os serviços nas quantidades estabelecidas no Anexo I.
- O serviço 0800 deverá possuir número único.
- O serviço 0800 deverá completar chamadas da modalidade local originadas de terminais fixos e móveis para o mesmo DDD da localidade da CONTRATANTE.
- São vedadas as chamadas de longa distância nacional, celular e longa distância internacional.
- O serviço 0800 deverão possuir as características de discagem gratuita na origem da chamada.
- A CONTRATANTE informará à CONTRATADA o tipo de interface (Acesso digital E1 ou linha analógica) especificado de acordo com o projeto de atendimento.
- O serviço deverá ser disponibilizado pela CONTRATADA 24 horas por dia, e estará limitado a escalas de atendimento e horários definidos pela CONTRATANTE.
- Central de Atendimento 24h por dia, 365 dias por ano através de um número 0800;

- Facilidades disponíveis:

• A utilização das facilidades deste item será objeto de aditivo contratual, pela CONTRATANTE.

- Agendamento por horário - permite ao CONTRATANTE especificar onde deverão terminar as chamadas em função do horário em que forem efetuadas.
- Agendamento por data - permite ao CONTRATANTE especificar onde as chamadas deverão terminar em função da data ou dia da semana em que serão realizadas para o número 0800.
- Seleção de origem - permite ao CONTRATANTE especificar para onde serão encaminhados os atendimentos (Centro de atendimento) das chamadas conforme a origem da ligação.
- Restrição de acesso por telefone público.
- Restrição de área de abrangência - permite ao CONTRATANTE bloquear as áreas das quais não deseja receber chamadas de telefones móveis.
- Mensagem Personalizada - permite ao CONTRATANTE definir conteúdo da mensagem que o chamador ouvirá ao ligar para o 0800.

- Prazo de transferência de endereço de instalação: até 30 dias.

- Distribuição Cíclica de Chamadas - distribui chamadas de modo uniforme, evitando a sobrecarga de um centro de atendimento ou atendente.
- Distribuição Sequencial de Chamadas - distribui sequencialmente as chamadas conforme ordem de troncos/ramais estabelecida, priorizando sempre a primeira terminação livre.

C) SERVIÇOS ESPECIAIS TRIDÍGITOS (UTILIDADE PÚBLICA): 153, 156, 192, 199

- Características mínimas:

- Fornecer os serviços nas quantidades estabelecidas no Anexo I.
- Os Serviços Especiais (Utilidade Pública) deverão possuir número único.
- Os Serviços Especiais (Utilidade Pública) deverão completar chamadas da modalidade local originadas de terminais fixos e móveis para o mesmo DDD da localidade da CONTRATANTE.
- São vedadas as chamadas de longa distância nacional, celular e longa distância internacionais.
- Os Serviços Especiais (Utilidade Pública) deverão possuir a característica de discagem gratuita na origem da chamada, com tarifação reversa, ou seja, por conta da CONTRATANTE.

- A CONTRATANTE informará à CONTRATADA o tipo de interface (Acesso digital E1 ou linha analógica) especificado de acordo com o projeto de atendimento.
- O serviço deverá ser disponibilizado pela CONTRATADA 24 horas por dia, e estará limitado a escalas de atendimento e horários definidos pela CONTRATANTE.
- Central de Atendimento 24h por dia, 365 dias por ano através de um número 0800.

- Prazo de transferência de endereço de instalação da linha atrelada ao Serviço Especial: até 10 dias úteis. Caso seja alterado o terminal ao qual está atrelado o Serviço Especial, o mesmo deverá ser cancelado e atribuído outro terminal compatível com a localidade onde será instalado o Serviço, com prazo também de até 10 dias úteis.

- Facilidades disponíveis:

• A utilização das facilidades deste item será objeto de aditivo contratual, pela CONTRATANTE.

- Agendamento por horário - permite ao CONTRATANTE especificar onde deverão terminar as chamadas em função do horário em que forem efetuadas.
- Agendamento por data - permite ao CONTRATANTE especificar onde as chamadas deverão terminar em função da data ou dia da semana em que serão realizadas para o número do Serviço Especial.
- Seleção de origem - permite ao CONTRATANTE especificar para onde serão encaminhados os atendimentos (Centro de Atendimento) das chamadas conforme a origem da ligação.
- Restrição de acesso por telefone público.
- Restrição de área de abrangência - permite ao CONTRATANTE bloquear as áreas das quais não deseja receber chamadas de telefones fixos ou móveis.
- Mensagem Personalizada - permite ao CONTRATANTE definir formato e conteúdo da mensagem que o chamador ouvirá ao ligar para os Serviços Especiais (Utilidade Pública).
- Distribuição Cíclica de Chamadas - distribui chamadas de modo uniforme, evitando a sobrecarga de um centro de atendimento ou atendente.
- Distribuição Sequencial de Chamadas - distribui sequencialmente as chamadas conforme ordem de troncos/ramais estabelecida, priorizando sempre a primeira terminação livre.

- Disponibilidade de instalação de novos códigos tridígitos homologados pela Anatel mediante solicitação da CONTRATANTE, no prazo máximo de 30 dias após a solicitação, em qualquer tipo de interface (analógica ou digital).

D) TRÁFEGO TELEFÔNICO:

Método

- Conforme especificações mínimas estabelecidas pelo órgão regulador.
- Informar os custos de mensalidade individuais das linhas telefônicas, troncos digitais, faixas DDR e Serviços Especiais (0800 e tridígitos).
- A tarifação das chamadas deverá ser realizada em minutos.
- As tarifas utilizadas deverão ter como base aquelas constantes do plano básico de serviços ou do plano alternativo de serviços, regulamentado para o setor de telecomunicação e informado através do preenchimento da Proposta Comercial, com todos os impostos regulamentados e descontos concedidos a critério da Licitante.

Perfil de tráfego

- Deverão ser considerados os volumes de chamadas indicadas no Anexo I, como referência orientativa para apresentação de proposta.
- O Perfil de Tráfego e seus custos (Anexo I) compõem-se de uma ESTIMATIVA, em minutos e em valores, baseada nas faturas das contas telefônicas da CONTRATANTE relativa às chamadas originadas em seu âmbito, bem como outros serviços atualmente utilizados.
- O Perfil de Tráfego do Anexo I servirá tão somente de subsídio para análise da proposta global mais vantajosa e, portanto, não implica em qualquer compromisso futuro ou restrição quantitativa de uso para a CONTRATANTE.

Da fatura

- As faturas de cada serviço devem ser encaminhadas via papel, individualizada por linha, com valor total e o respectivo descritivo com os valores das ligações.

Do reajuste

- O reajuste das tarifas será de acordo com o poder concedente e com data e índice determinado pela ANATEL.

Do atendimento à CONTRATANTE

- A contratada deverá disponibilizar atendimento VIP por um Gerente de Contas e/ou Gerente de Negócios Corporativos da área comercial da CONTRATADA visando a agilização dos atendimentos das demandas da CONTRATANTE.

E) LINHAS TELEFÔNICAS ANALÓGICAS:

- Fornecer linhas telefônicas analógicas nas quantidades e endereços estabelecidos no Anexo I.
- Ativar novas linhas telefônicas conforme necessidade da CONTRATANTE.
- Desativar linhas telefônicas que estiverem em operação conforme necessidade da CONTRATANTE.
- Possibilidade de serviços adicionais como identificador de chamadas, busca entre terminais, serviço ADSL, bloqueio de ligações a cobrar ou DDD, DDI e celular conforme necessidade da CONTRATANTE.
- Novas linhas telefônicas deverão ser instaladas no prazo máximo contratual de 10 dias úteis, com possibilidade desconto de 100% na tarifa de instalação.
- Devem ser tele-alimentadas, a fim de garantir a comunicação mesmo na falta de energia elétrica.
- Tecnologias alternativas como WLL (Wireless Local Loop) e FWT (Fixed Wireless Terminal) serão permitidas somente para endereços rurais ou muito afastadas da cidade ou bairros novos.
- Central de Atendimento 24h por dias, 365 dias por ano através de um número 0800 ou similar gratuito.
- A CONTRATADA deverá manter a mesma numeração atualmente utilizada (números de telefone) conforme critérios da Portabilidade regulamentada pela ANATEL.
- As linhas analógicas individuais deverão permitir serviço de conexão do tipo banda larga e comunicação de dados MPLS para integrar a rede de dados da Prefeitura Municipal e suas

localidades remotas, resguardada a segurança e a inviolabilidade por terceiros não autorizados pela Prefeitura, sem prejuízo da qualidade dos serviços de voz.

- As linhas analógicas individuais devem suportar os Serviços Especiais de Utilidade Pública (199, 153, 156, etc.), sem custo para a contratante.

- As linhas analógicas deverão comportar, mediante análise prévia da contratada, os serviços de Busca Automática, Identificador de Chamadas, Bloqueador de Celular ou, Bloqueador de Interurbanos e serviços afins, que deverão ser ofertados pela CONTRATADA mediante solicitação da CONTRATANTE, com a cobrança das tarifas praticadas no mercado por ocasião do certame licitatório.

F) DO LINK DEDICADO:

1. O serviço de fornecimento de acesso à Internet link Dedicado, objeto deste termo de referência, deverá ser disponibilizado ao endereço discriminado na tabela deste anexo.

2. Os serviços serão executados conforme as especificações abaixo:

1. **VELOCIDADE DE ACESSO:** 2(dois) acessos sendo um de 20(vinte) e outro de 80(oitenta) Mbps, de forma simétrica e dedicada.

2. **DISPONIBILIDADE:** 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, durante todo o ano.

3. **MEIO DE TRANSMISSÃO:** por fibra óptica fim a fim.

4. **ACESSO ILIMITADO:** Não deverá haver franquia de consumo mensal, podendo a CONTRATADA utilizar tanto tráfego, seja de *download* como de *upload*, quanto lhe permita o link contratado. Não deverá haver corte no fornecimento do serviço nem limitação de velocidade abaixo da contratação, por maior que seja a quantidade de Gigabytes transferidos através do link durante o mês.

5. **MODELAGEM DE TRÁFEGO:** O link poderá ser utilizado pelo CONTRATANTE para o tráfego de dados, voz e vídeo em sua velocidade máxima, sem que haja qualquer modelagem de tráfego (*traffic shaping*) controlada pela CONTRATADA, que venha a priorizar um determinado tipo de comunicação em detrimento de outro, seja bloqueando, retardando ou diminuindo seu tráfego sem o pedido ou consentimento do CONTRATANTE.

6. **CONFIGURAÇÃO, GERENCIAMENTO E MONITORAMENTO:** Deverão ser disponibilizadas ferramentas *on line* de configuração, gerenciamento, monitoramento e atendimento ao usuário contemplando, no mínimo, as seguintes funções:

– **GERÊNCIA DE DESEMPENHO/CAPACIDADE:** função que permita aferir se as taxas de dados fornecidas são compatíveis com o serviço contratado e apresente gráficos com análise de tráfego com periodicidade diária;

– **GERÊNCIA DE FALHAS/INDISPONIBILIDADE:** função que permita identificar taxas de erros e perda de pacotes, intermitência e queda de enlace/link (disponibilidade), além do acompanhamento dos chamados técnicos;

– **GERÊNCIA DE CONFIGURAÇÃO:** função que forneça dados informativos e permita a configuração dos equipamentos gerenciados, conexões físicas e lógicas, e disponibilize *logs* de sistema para análise de falhas; e

– **ATENDIMENTO AO USUÁRIO:** função que permita a abertura e consultas de registros de ocorrências (chamadas), em língua portuguesa, devido as indisponibilidades, falhas ou baixa qualidade dos serviços através de Central de Atendimento, seja por telefone franqueado (0800) ou via portal *Web*, com números de protocolo para que seja possível acompanhamento dos mesmos.

1.1 A CONTRATADA deverá executar o serviço utilizando-se dos materiais, equipamentos, ferramentas e utensílios necessários à perfeita execução contratual, conforme disposto neste Termo de Referência.

1.2 A aquisição, instalação e configuração dos equipamentos necessários à prestação do serviço serão responsabilidade da CONTRATADA.

1.3 Toda a conexão entre o *backbone* da CONTRATADA e os equipamentos a serem instalados por ela nas dependências do órgão, serão de responsabilidade da mesma.

1.4 Deverão ser fornecidos, no mínimo, 4 (quatro) números de endereços IP (*Internet Protocol*) fixos e válidos.

Os equipamentos integrantes do serviço ofertado pela licitante necessários à entrega do link de acesso à Internet no local de instalação deverão:

1.4.1 Os equipamentos necessários para a entrega do link não integrarão o patrimônio do órgão e deverão ser recolhidos pela Contratada ao final do contrato.

1.4.2 A responsabilidade de configuração dos equipamentos será da Contratada.

1.4.3 Permitir gerenciamento via *SNMP v3*, para que o órgão realize monitoramento.

1.4.4 Deverá ser disponibilizada *community SNMP de read* para que o 3º CTA possa monitorar o enlace.

1.4.5 Possuir suporte à pilha de protocolos *TCP/IP*.

1.4.6 Possuir suporte a *Internet Control Message Protocol (ICMP)*.

1.4.7 Permitir configuração de facilidades e regras de roteamento através de console local e remotamente com *SSH*.

1.4.8 Efetuar filtragem de pacotes por endereço de origem, endereço de destino, porta de origem, porta de destino e protocolos.

1.4.9 Possuir suporte ao protocolo *HSRP*, ou protocolo com funções equivalentes,

- 1.4.10 para a realização de redundância.
- 1.4.11 Possuir fontes de alimentação de 110/220 VCA com chaveamento automático ou manual.
- 1.4.12 Suportar o enlace contratado.
- 1.4.13 Os equipamentos deverão vir acompanhados de todos os softwares, cabos e acessórios para permitir o seu perfeito funcionamento e montagem conforme o especificado neste Termo de Referência.
- 1.4.14 Suportar passagem de pacotes VPN com protocolo IPSEC e SSL.

NÍVEIS DE SERVIÇO E MÉTODOS DE AVALIAÇÃO

1. Devido à necessidade de manter a elevada disponibilidade e qualidade dos serviços que serão providos pelo órgão, o serviço de acesso à Internet contratado deverá ser executado com base nos parâmetros mínimos estabelecidos a seguir.
 2. O Índice de Disponibilidade Mensal (**D**) de cada porta do ponto de acesso será de no mínimo 99,2% (noventa e nove vírgula dois por cento).
 3. O Índice de Disponibilidade Anual de cada porta do ponto de acesso será de 99,3% (noventa e nove vírgula três por cento). Entende-se por Disponibilidade Anual a média das Disponibilidades mensais, descritas no item 4.2, por um período de 12 (doze) meses contados a partir do início da vigência do contrato.
1. Não serão consideradas indisponibilidades as seguintes situações:
 - Paradas programadas pela CONTRATADA para fins de manutenção preventiva ou corretiva, solicitadas com antecedência de, pelo menos, 10 (dez) dias úteis e aprovadas pelo órgão. Essas interrupções serão realizadas nos finais de semana ou em feriados;
 - Paradas ocasionadas por problemas internos do órgão, sem responsabilidade da CONTRATADA.
 1. Ficam também estabelecidos limites de tolerância para os percentuais de disponibilidade calculados que, ao serem excedidos, determinarão glosas específicas nos custos das portas de comunicação, conforme a tabela a seguir:

Limite	Penalidade
Disponibilidade entre 98,0% e 99,29%	Glosa de 5% (cinco por cento) do custo mensal do canal de comunicação.
Disponibilidade entre 98,0% e 97,0%	Glosa de 7% (setenta por cento) do custo mensal do canal de comunicação.
Disponibilidade inferior a 97,0%	Glosa de 10% (cem por cento) do custo mensal do canal de comunicação.

1. A aplicação das glosas nos custos das portas de comunicação não dispensa a CONTRATADA das eventuais penalidades previstas em contrato, em virtude

do descumprimento das exigências relativas aos índices de disponibilidade do ponto de acesso.

- 1 O padrão de qualidade SLA deverá ser, no máximo, de 50 ms em relação ao índice de Latência (em milissegundos).
- 2 O padrão de qualidade SLA deverá ser, no máximo, de 1% em relação ao índice de Perda de Pacotes.
- 3 Dois meses consecutivos de não cumprimento da garantia de desempenho obrigarão a CONTRATADA a conceder crédito ao CONTRATANTE, correspondente a 01 (um) dia de Prestação de Serviço, equivalente a 1/30 do preço mensal pago pelo serviço definido no contrato.
- 4 O serviço de comunicação de dados será considerado indisponível quando ocorrer qualquer tipo de problema nos pontos de acessos – nos Equipamentos de Comunicação de Dados e/ou no enlace de comunicação de responsabilidade da CONTRATADA – que impeça a transmissão ou a recepção de pacotes através deles.
- 5 Também será considerado indisponível o serviço de comunicação de dados quando houver uma perda de pacotes superior a 2% num período contínuo de 30 (trinta) minutos. Para o cálculo deste parâmetro não serão considerados pacotes descartados em função do esgotamento da capacidade do link, situações definidas quando a utilização for superior a 90% (noventa por cento) da taxa contratada.
- 6 Mensalmente, acompanhada das notas fiscais de faturamento, a CONTRATADA deverá apresentar relatórios referentes aos períodos de indisponibilidade de cada uma das portas de comunicação, mantendo também esses dados disponíveis em seus Portais Eletrônicos de Acompanhamento dos Serviços.
- 7 Sempre que forem apurados percentuais de disponibilidade que estejam abaixo dos limites mínimos estabelecidos, o somatório dos tempos de indisponibilidade dentro do período de faturamento serão descontados dos custos mensais dos serviços.

SUPORTE TÉCNICO

1 A CONTRATADA responderá por todos os vícios e defeitos dos serviços durante o período de vigência do contrato.

2 O suporte técnico deverá estar disponível 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

3 A abertura e acompanhamento de chamados técnicos deverá ser disponibilizada ao órgão pela CONTRATADA por meio de telefone 0800, e-mail, e área em página da Web, os quais serão informados ao CONTRATANTE no início da vigência do contrato.

4 O suporte técnico poderá ser prestado inicialmente de forma remota. Persistindo o problema, a CONTRATADA deverá enviar um técnico ao local de instalação do link.

5 O suporte técnico ocorrerá sem qualquer ônus para o CONTRATANTE, mesmo quando for necessária a troca de equipamentos da CONTRATADA, o traslado e a estada de técnicos da CONTRATADA ou qualquer outro tipo de serviço necessário para garantir o cumprimento do serviço.

6 A CONTRATADA somente realizará o fechamento de um chamado depois que um técnico do órgão confirmar a solução do problema relacionado ao chamado.

7 As manutenções e interrupções deverão obedecer aos seguintes procedimentos:

- Caso haja a necessidade de realizar manutenção preventiva com a presença de um técnico da CONTRATADA nas instalações do CONTRATANTE, a CONTRATADA deverá avisar com 10 (dez) dias de antecedência da data proposta para a realização do serviço, que deverá ser ratificada por um dos membros da equipe técnica do CONTRATANTE; e
- Em caso de necessidade de interrupção do serviço, a CONTRATADA deverá entrar em contato com o CONTRATANTE com antecedência mínima de 10 (dez) dias úteis;

8 O prazo máximo para a solução de qualquer problema de inoperância, a partir do momento da comunicação formal da CONTRATANTE à CONTRATADA, respeitados os índices de disponibilidade mensal e de disponibilidade anual estabelecidos acima, deverá ser de:

- até **6 (seis) horas**, quando referente aos circuitos do ponto de acesso, seja o problema decorrente de defeito físico do próprio circuito ou de configuração de equipamentos de comunicação de dados; prorrogáveis mediante justificativa .
- até **8 (oito) horas**, quando acarretar na substituição de componentes de *hardware*, prorrogáveis mediante justificativa .

9 Com relação à prestação de esclarecimentos técnicos: o CONTRATANTE poderá solicitar formalmente esclarecimentos técnicos relativos às ocorrências, aos dados de gerência, ao uso e ao aprimoramento dos serviços, ficando a CONTRATADA obrigada a responder os questionamentos no prazo máximo de 20 (vinte) dias úteis.

DO LINK BANDA LARGA:

1.O serviço de fornecimento de acesso à Internet banda larga, objeto deste termo de referência, deverá ser disponibilizado conforme quantidades estabelecidas na tabela deste anexo com velocidades discriminadas.

2.O serviço poderá ter a instalação nos meios físicos: fibra ótica , par metálico.

3.Os serviços serão executados conforme as especificações abaixo:

3.1.VELOCIDADE DE ACESSO: conforme tabela .

3.2.DISPONIBILIDADE: 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, durante todo o ano.

3.3.MEIO DE TRANSMISSÃO: Transmissão por fibra óptica ou par metálico.

4.A instalação ocorrerá no prazo máximo de até 07 (sete) dias, contados da data da ordem de serviço emitida pela **CONTRATANTE**.

5.Visita Técnica para fins de reparação ocorrerá no prazo máximo de 48 (quarenta e oito) horas, contados da data da solicitação do **CLIENTE**.

6.CONDIÇÕES ESPECIAIS:

6.1.A CONTRATADA obriga-se a executar os serviços em perfeita harmonia e concordância com as normas adotadas pela CONTRATANTE, com especial observância dos termos deste contrato.

7. INFRAESTRUTURA NECESSÁRIA À PRESTAÇÃO INTERNET Banda Larga

7.1.Para a disponibilização e regular funcionamento da **INTERNET Banda Larga**, faz-se necessário que a **CONTRATANTE** disponibilize:

7.1.1. Um micro computador com seus acessórios, que devem obedecer às especificações técnicas indicadas pela **contratada**,

7.1.2.A **CONTRATADA** cederá a Prefeitura o modem (XDSL) em regime de comodato para a prestação do serviço XDSL **INTERNET Banda Larga** .

7.1.3.As velocidades contratadas na **INTERNET Banda Larga** são velocidades nominais máximas de acesso, sendo que estão sujeitas a variações decorrentes da própria tecnologia utilizada e das redes que compõem a Internet, conforme os fatores técnicos que podem interferir na velocidade contratada:

7.1.3.1.A **CONTRATADA** fornecerá velocidade instantânea mínima nos termos da Resolução **574/2011 – Anatel**.

8.Para a instalação do **INTERNET Banda Larga** a contratada fará uma avaliação técnica previa do endereço de instalação podendo não haver viabilidade técnica para fornecimento do serviço.

9.Os equipamentos integrantes do serviço ofertado pela licitante necessários à entrega do link de acesso à Internet no local de instalação deverão:

9.1.1.Os equipamentos necessários para a entrega do link não integrarão o patrimônio do órgão e deverão ser recolhidos pela Contratada ao final do contrato.

9.1.2.A responsabilidade de configuração dos equipamentos será da Contratada.

SUPORTE TÉCNICO

1 A CONTRATADA responderá por todos os vícios e defeitos dos serviços durante o período de vigência do contrato.

2 A abertura de chamado técnico poderá ocorrer em qualquer horário e dia, e caso haja necessidade de visita técnica, essa será efetuada somente em horário comercial.

3 A abertura e acompanhamento de chamados técnicos deverá ser disponibilizada ao órgão pela CONTRATADA por meio de telefone 0800, e-mail, e área em página da Web, os

quais serão informados ao CONTRATANTE no início da vigência do contrato.

4 O suporte técnico poderá ser prestado inicialmente de forma remota. Persistindo o problema, a CONTRATADA deverá enviar um técnico ao local de instalação do link.

5 O suporte técnico ocorrerá sem qualquer ônus para o CONTRATANTE, ressalvo quando for necessária a troca de equipamentos da CONTRATADA.

6 A CONTRATADA somente realizará o fechamento de um chamado depois que um técnico do órgão confirmar a solução do problema relacionado ao chamado.

7 As manutenções e interrupções deverão obedecer aos seguintes procedimentos:

- Caso haja a necessidade de realizar manutenção preventiva com a presença de um técnico da CONTRATADA nas instalações do CONTRATANTE, a CONTRATADA deverá avisar com 10 (dez) dias de antecedência da data proposta para a realização do serviço, que deverá ser ratificada por um dos membros da equipe técnica do CONTRATANTE; e

- Em caso de necessidade de interrupção do serviço, a CONTRATADA deverá entrar em contato com o CONTRATANTE com antecedência mínima de 10 (dez) dias úteis;

8 O prazo máximo para a solução de qualquer problema de inoperância, a partir do momento da comunicação formal da CONTRATANTE à CONTRATADA, respeitados os índices de disponibilidade mensal e de disponibilidade anual estabelecidos acima, deverá ser de:

- até **24 (vinte e quatro) horas**, quando referente aos circuitos do ponto de acesso, seja o problema decorrente de defeito físico do próprio circuito ou de configuração de equipamentos de comunicação de dados;

9 Com relação à prestação de esclarecimentos técnicos: o CONTRATANTE poderá solicitar formalmente esclarecimentos técnicos relativos às ocorrências, aos dados de gerência, ao uso e ao aprimoramento dos serviços, ficando a CONTRATADA obrigada a responder os questionamentos em um prazo de até 20 (vinte) dias úteis.

2 - SERVIÇO GERENCIADO DE SEGURANÇA MSS

1 DESCRIÇÃO DO SERVIÇO - ESPECIFICAÇÕES DOS SERVIÇOS DA SOLUÇÃO

Contratação de empresa especializada para fornecimento de **MSS** (*Managed Security Services*) sobre a solução de segurança com as funcionalidades descritas em **ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO**, contemplando serviços de instalação, configuração, manutenção, suporte técnico remoto, monitoramento e gerenciamento na modalidade 24x7x365.

CARACTERÍSTICAS DOS SERVIÇOS

1.1. Solução de Gerenciamento com fornecimento de hardware e software

1.1.1. A **CONTRATADA** deverá fornecer, em regime de **comodato**, conforme descrito em **ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO**, necessária para a realização dos serviços, em regime 24x7x365 para a solução ofertada durante a vigência do contrato.

1.1.1.1. A solução de hardware e software deverá ser compatível com o ambiente operacional da **CONTRATANTE**.

1.1.1.2. A **CONTRATADA** será responsável pela manutenção preventiva e corretiva da solução de hardware e software, sem qualquer ônus para a **CONTRATANTE**.

1.2. Gerenciamento/Manutenção

1.2.1. O gerenciamento deverá ser em regime de operação 24 (vinte e quatro) horas por dia e 07 (sete) dias por semana, inclusive feriados, sobre os serviços, garantindo o melhor resultado nas aplicações da **CONTRATANTE** e deverá abranger as atividades de manutenção, supervisão e administração.

1.3. Serviço de comunicação de dados

1.3.1. A **CONTRATADA** deverá realizar as configurações necessárias para interligação de seu SOC (*Security Operation Center* - Centro de Operações de Segurança) às instalações do **CONTRATANTE**, por meio de uma linha de comunicação privativa de dados (LP) ou através de uma VPN IPsec, com a finalidade exclusiva de realizar a prestação do serviço, durante a vigência do contrato.

1.3.2. Todo acesso de monitoração do ambiente, e eventuais intervenções remotas, pela **CONTRATADA** deverão ser feitos exclusivamente por esse serviço de comunicação de dados.

1.4. Infraestrutura mínima necessária.

1.4.1. Para prestação de serviço de monitoramento remoto de segurança lógica, a **CONTRATADA** deverá utilizar um Centro de Operações de Segurança – SOC (*Security Operation Center*) próprio com redundância, localizado no Brasil, com certificação ISO 27000.

1.4.2. Os processos utilizados pela equipe do SOC devem seguir as melhores práticas de mercado. O ITIL (*Information Technology Infrastructure Library*), ISO 27001 (*Information security incident management*) deve ser utilizado como modelo de referência pelo SOC para operação e gerenciamento de processos e serviços de TI.

1.4.3. Responsabilidades do SOC

1.4.3.1. A Infraestrutura do SOC da **CONTRATADA** deve possuir mecanismos de segurança física e lógica necessários para garantir a segurança das informações e do ambiente operacional, incluindo:

- 1.4.3.1.1. Segurança física: mecanismos de monitoração e registro de todo e qualquer acesso ao SOC, utilizando-se de câmeras de segurança;
- 1.4.3.1.2. Acesso ao SOC controlado por mecanismos de autenticação forte (pelo menos autenticação de dois fatores); ambiente isolado de outros que não sejam destinados à operacionalização e controle de segurança;
- 1.4.3.1.3. Mecanismos de prevenção, detecção e combate a incêndios;
- 1.4.3.1.4. Política de acesso lógico: possuir autenticação forte no acesso aos equipamentos que estarão nas dependências da **CONTRATANTE**, com usuários segregados por função e registros para controle de auditoria;
- 1.4.3.1.5. Possuir políticas definidas para criação, exclusão e manutenção de chaves, senhas e perfis de acesso.

1.4.4. O SOC da **CONTRATADA** deve possuir competência para a prestação de serviços, sendo:

1.4.4.1. MANUTENÇÃO

- 1.4.4.1.1. Fornecer apoio técnico necessário para realizar o diagnóstico de eventos de falha em seus ativos de segurança. Através da análise dos logs do equipamento, o SOC deverá determinar se houve alguma avaria em um dos componentes de hardware da solução e identificar a necessidade ou não de sua substituição.
- 1.4.4.1.2. Efetuar o processo de RMA (sigla em inglês de *return merchandise authorization*).

- 1.4.4.1.3. Efetuar quando necessário toda a interface com o fabricante, para o RMA e substituição do componente danificado.

1.4.4.2. SUPERVISÃO

- 1.4.4.2.1. Efetuar a monitoração constante da capacidade e da disponibilidade da infraestrutura de segurança contratada.
- 1.4.4.2.2. Compreender as atuais demandas sobre os recursos de segurança e criar previsões para futuras solicitações quando necessário.
- 1.4.4.2.3. Avaliar se o nível de disponibilidade é sustentável, permitindo o negócio atingir seus objetivos de forma consistente.
- 1.4.4.2.4. Ter uma arquitetura de monitoração, baseada em solução que utiliza o protocolo SNMP para realizar os *healthchecks*.
- 1.4.4.2.5. Processar e disponibilizar em relatórios mensais os dados coletados.
- 1.4.4.2.6. Identificar que o componente atingiu certo nível de utilização (threshold).
- 1.4.4.2.7. Alertar e encaminhar para os técnicos responsáveis pela administração.
- 1.4.4.2.8. Acompanhar a saúde dos dispositivos supervisionando-os 24 horas / dia x 7 dias por semana.
- 1.4.4.2.9. Comunicar ao CONTRATANTE, anomalias quando um componente monitorado apresentar índices não usuais.
- 1.4.4.2.10. Prover a monitorização da saúde dos dispositivos através de um número predefinido de itens, conforme abaixo:
 - 1.4.4.2.10.1. Utilização da CPU;
 - 1.4.4.2.10.2. Utilização de memória;
 - 1.4.4.2.10.3. Utilização do disco;
 - 1.4.4.2.10.4. Estado das interfaces de rede;
 - 1.4.4.2.10.5. Temperatura;
 - 1.4.4.2.10.6. Número de sessões de VPN;
 - 1.4.4.2.10.7. Número de pacotes perdidos;
 - 1.4.4.2.10.8. Número de pacotes negado;
 - 1.4.4.2.10.9. Número de conexões;
 - 1.4.4.2.10.10. Estado do cluster;
 - 1.4.4.2.10.11. Estado de serviços.
- 1.4.4.2.11. Estas verificações serão ativadas no momento de implantação do serviço, utilizando definições padrão de *thresholds*.

- 1.4.4.2.12. Estes valores poderão ser ajustados caso necessário, a fim de identificar quais situações normalmente não correspondem à normalidade dos serviços.

1.4.4.3. ADMINISTRAÇÃO

- 1.4.4.3.1. Realizar a operação remota, gestão de mudança e gestão de configuração dos dispositivos de segurança contratado.
- 1.4.4.3.2. Resolução nos incidentes de segurança que ocorrem nos elementos administrado (s), detectados pelo monitoramento ou que sejam informados pela CONTRATANTE.
- 1.4.4.3.3. Planejar e realizar implementação de mudanças no ambiente contratado e gerenciado, sejam elas solicitadas pelo **CONTRATANTE** ou mesmo por recomendação da própria **CONTRATADA**, baseados nas melhores práticas de gestão.
- 1.4.4.3.4. Efetuar tarefas operacionais básicas, tais como executar *backup/restore* de configurações e gerenciamento do ambiente contratado.
- 1.4.4.3.5. Garantir o correto funcionamento dos dispositivos administrados.
- 1.4.4.3.6. Manter e atualizar o ambiente contratado com o software do dispositivo na versão mais atual recomendada pelo fabricante.
- 1.4.4.3.7. Efetuar aplicação de patches para a resolução de incidentes, correção de vulnerabilidades e prevenção de incidentes de segurança.
- 1.4.4.3.8. Efetuar atualização de software e patches somente se e quando autorizada pela **CONTRATANTE**, através do processo de gestão da mudança.
- 1.4.4.3.9. Informar ao **CONTRATANTE** dos possíveis riscos de segurança identificados através da administração da infraestrutura ou através das ferramentas de administração.
- 1.4.4.3.10. Atender as dúvidas e solicitações de segurança da **CONTRATANTE**.
- 1.4.4.3.11. Acompanhar e encaminhar os chamados através de ferramenta.

1.5. Implantação da Solução:

- 1.5.1. A implantação da solução de hardware e software deverá ser realizada no prazo de até **60 (sessenta)** dias da contratação, mediante entrega de cronograma, detalhando as fases do projeto de implantação. Esse cronograma

deverá ser aprovado pelo **CONTRATANTE**, sendo a implantação iniciada somente após esta aprovação.

1.5.2. As fases do projeto, bem como os respectivos documentos mínimos necessários para cada fase, estão descritas a seguir:

1.5.2.1. Projeto: Relatório de organização e planejamento, matriz de responsabilidade, modelos de atuação, plano de resposta a incidentes e plano de comunicação;

1.5.2.2. Implantação: Relatório de implantação;

1.5.2.3. Testes: Relatório de testes, com evidências de sucesso e falhas.

1.5.3. A implantação da solução será realizada pela **CONTRATADA** e o planejamento e a execução de todas as atividades envolvidas serão acompanhados, autorizados e coordenados por servidores designados pela **CONTRATANTE**.

1.5.4. A implantação da solução, quando realizada no ambiente de produção, poderá envolver, a critério da **CONTRATANTE**, atividades fora do horário de expediente (horários noturnos ou em finais de semana e feriados).

1.5.5. A **CONTRATADA** será responsável por efetuar as atividades de integração da solução ofertada com o ambiente operacional da **CONTRATANTE**, sem provocar qualquer prejuízo aos serviços desta.

1.5.6. Após a implantação da solução e estando tudo de acordo com este Termo de Referência, a **CONTRATANTE** irá emitir o termo de aceite da implantação.

1.5.7. A infraestrutura para instalação desta solução (energia elétrica, rack para acomodar equipamentos, cabeamento estruturado, sistema de refrigeração, entre outros) é de responsabilidade da contratante.

2. PRESTAÇÃO DOS SERVIÇOS

2.1. Os serviços serão realizados pela **CONTRATADA** na modalidade 24x7x365 (vinte e quatro horas por dia, sete dias na semana, 365 dias por ano).

2.2. Controle dos Serviços Realizados pela **CONTRATADA**

2.2.1. Para o controle e administração dos serviços realizados pela **CONTRATADA**, a **CONTRATANTE** indicará pelo menos 02 (dois) representantes autorizados a interagir com aquela. Tais representantes serão responsáveis por:

2.2.1.1. Manter as informações técnicas (configuração do ambiente) atualizadas, bem como dar suporte na implantação e manutenção da solução;

- 2.2.1.2. Definir as estratégias, políticas e regras a serem implantadas, e analisar/aprovar as solicitações;
 - 2.2.1.3. Tomar as providências necessárias, em caso da ocorrência de algum incidente (análise dos logs, rastreamento da ocorrência).
 - 2.2.2. A **CONTRATANTE** poderá realizar inspeção nas instalações do SOC, com o objetivo de verificar a segurança física e lógica do ambiente, a qualquer tempo com a **CONTRATADA**.
- 2.3. Ocorrência de Incidentes
- 2.3.1. No caso de detecção de algum incidente de segurança, a **CONTRATADA** deverá notificar a **CONTRATANTE** dentro do período estabelecido no SLA, para que sejam tomadas as medidas corretivas e legais necessárias.
 - 2.3.1.1. São considerados incidentes de segurança: os acessos indevidos, instalação de códigos maliciosos, ataques por força bruta, ou qualquer outra ação que vise prejudicar a funcionalidade ou a disponibilidade dos serviços da **CONTRATANTE**.
 - 2.3.2. A **CONTRATADA** comunicará imediatamente a **CONTRATANTE**, para que possam ser tomadas ações preventivas, nos casos de tentativas, sem sucesso, de acessos indevidos, de instalação de códigos maliciosos, ou de qualquer outra ação que venha pôr em risco a segurança do ambiente do **CONTRATANTE**, em que seja evidenciada a insistência, por parte da pessoa mal-intencionada.
 - 2.3.3. A **CONTRATADA** disponibilizará todas as informações necessárias (origem do ataque, tipo de ataque, data e hora, logs, etc.) para que sejam apurados os incidentes de segurança reportados junto ao ambiente contratado.
- 2.4. Encerramento dos Serviços de Monitoração Remota da Segurança
- 2.4.1. Quando do encerramento da prestação do serviço de monitoração remota da segurança, a **CONTRATADA** retirará os componentes da solução.
 - 2.4.2. Todas as informações de customização, políticas e regras, logs de auditoria serão disponibilizadas para a **CONTRATANTE** e, em seguida, eliminadas da base de dados da **CONTRATADA**.
- 2.5. Confidencialidade da Informação.
- 2.5.1. Todas as informações que trafegam nos equipamentos, bem como todas e quaisquer informações originadas pela **CONTRATANTE**, que a
 - 2.5.2.

CONTRATADA venha a ter acesso serão consideradas “Informações Confidenciais”.

- 2.5.3. A **CONTRATADA** se compromete a guardar confidencialidade e a não utilizar qualquer tipo de Informação Confidencial para propósitos estranhos àqueles definidos neste Termo de Referência ou em benefício próprio ou de terceiros.
- 2.5.4. A **CONTRATADA** se compromete a adotar as medidas necessárias para que seus dirigentes, empregados, e em geral todas as pessoas que trabalham sob sua responsabilidade, que precisem conhecer a Informação Confidencial, mantenham a confidencialidade acordada neste instrumento, sendo responsável pela ruptura do compromisso de confidencialidade pelos seus empregados.
- 2.5.5. A **CONTRATADA** se obriga a devolver ou destruir imediatamente todo o material que contenha Informações Confidenciais, tão logo ocorra a rescisão ou término da vigência do contrato firmado entre as partes.
- 2.5.6. A **CONTRATANTE** também se compromete a tratar como confidenciais todas as informações de propriedade da **CONTRATADA**, que vier a ter conhecimento, durante a vigência do contrato.

3. ACORDO DE NÍVEIS DE SERVIÇO – SLA (*SERVICE LEVEL AGREEMENT*)

3.1. SLO (*Service Level Objectives* - Objetivos de Nível de Serviço) para serviços gerenciados

- 3.1.1. Os SLO's serão estabelecidos de acordo com a severidade do incidente ocorrido, conforme descrito no quadro abaixo:

Incidentes de Serviço	Definição
Crítico	Evento que indisponibiliza os serviços de um ativo classificado como crítico
Alto	Evento que degrada os serviços de um ativo classificado como crítico ou que indisponibiliza os serviços de um ativo não crítico
Médio	Evento que degrada os serviços de um ativo classificado como não crítico
Baixo	Evento que não afeta os serviços

3.1.2. Abaixo os tempos de atendimento:

Serviço	Definição	Crítico	Alto	Médio	Baixo
Todos	Tempo de atendimento a partir da comunicação do cliente até a atribuição do ticket a um analista do SOC	30 min.	1h.	2h.	4h.
Todos	Tempo de resposta a partir da comunicação do cliente até que SOC faça o primeiro diagnóstico	1,5h.	2h.	4h.	8h.
Todos	Tempo de resolução a partir da comunicação do cliente até que o SOC comunique a resolução do mesmo	4h.	6h.	12h.	24h.

3.1.3. SLO de Solicitações e Consultas:

Serviço	Definição	Alto	Médio	Baixo
Todos	Tempo de atendimento a partir da comunicação do cliente até a atribuição do ticket a um analista do SOC	2h.	4h.	5h.
Todos	Tempo de resolução a partir da comunicação do cliente até que o SOC comunique a resolução do mesmo	16h.	20h.	30h.

ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO

3.2. SOLUÇÃO DE SEGURANÇA DE REDE

- 3.3. O *Unified Threat Management* (UTM), para proteção de informação perimetral e de rede interna que inclui *stateful firewall* com capacidade de controle de tráfego de dados por identificação de usuários, controle de aplicação, administração de largura de banda (QoS), VPN IPsec e SSL, IPS, prevenção contra ameaças de vírus, *malwares*, Filtro de URL, inspeção de tráfego criptografado. Deverá ser fornecida em hardware específico.
- 3.4. O hardware e o software fornecidos não podem constar, no momento da apresentação da proposta, em listas de *end-of-sale*, *end-of-support*, *end-of-engineering-support* ou *end-of-life* do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante.

4 QUANTIDADES PREVISTAS

Aquisição de solução de segurança UTM e Access Point, compreendendo aquisição de equipamentos (hardwares), softwares e prestação de serviços, conforme tabela abaixo:

Item	Descrição	Quantidade
HARDWARE		
1	Solução em cluster de Firewall UTM/NGFW	2 unidade
SOFTWARE		
2	Pacote de licenças de NG Firewall, IPS, Antivírus, AntiSpam, Filtro de Web.	2 unidade

5 CARACTERÍSTICAS ESPECÍFICAS DE DESEMPENHO E HARDWARE DA SOLUÇÃO DE FIREWALL

- 5.1 Throughput de, no mínimo, 4.4 Gbps com a funcionalidade de firewall habilitada para tráfego IPv4 e IPv6, independentemente do tamanho do pacote.
- 5.2 Suporte a, no mínimo, 2 Milhões conexões simultâneas.
- 5.3 Suporte a, no mínimo, 30.000 novas conexões por segundo.
- 5.4 Throughput de, no mínimo, 4 Gbps de VPN IPsec.
- 5.5 Estar licenciado para ou suportar sem o uso de licença, 2.000 túneis de VPN IPSEC Site-to-Site simultâneos.

- 5.6 Estar licenciado para ou suportar sem o uso de licença, 10.000 túneis de clientes VPN IPSEC simultâneos.
- 5.7 Throughput de, no mínimo, 250 Mbps de VPN SSL.
- 5.8 Suporte a, no mínimo, 300 clientes de VPN SSL simultâneos.
- 5.9 Suportar no mínimo 500 Mbps de throughput de IPS.
- 5.10 Suportar no mínimo 190 Mbps de throughput de Inspeção SSL
- 5.11 Throughput de, no mínimo, 250 Mbps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS, Antivírus e Antispyware. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito;
- 5.12 Permitir gerenciar no mínimo 32 Access Points.
- 5.13 Possuir ao menos interface, 20xGE RJ45.
- 5.14 Estar licenciado e/ou ter incluído sem custo adicional, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance.

6 CARACTERÍSTICAS GERAIS PARA SOLUÇÃO DE FIREWALL

- 6.1 A solução deve consistir em plataforma de proteção de rede baseada em appliance com funcionalidades de Next Generation Firewall (NGFW), e console de gerência e monitoração;
- 6.2 Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;
- 6.3 As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação;
- 6.4 A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;
- 6.5 Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19”, incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;
- 6.6 O software deverá ser fornecido em sua versão mais atualizada;
- 6.7 O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API

aberta;

6.8 O gerenciamento da solução deve suportar a interface de administração via web no próprio dispositivo de proteção de rede

6.9 Os dispositivos de proteção de rede devem possuir suporte a 4094 VLAN Tags 802.1q;

6.10 Os dispositivos de proteção de rede devem possuir suporte a agregação de links 8023ad e LACP;

6.11 Os dispositivos de proteção de rede devem possuir suporte a Policy based routing ou policy based forwarding;

6.12 Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);

6.13 Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay;

6.14 Os dispositivos de proteção de rede devem possuir suporte a DHCP Server;

6.15 Os dispositivos de proteção de rede devem suportar sFlow;

6.16 Os dispositivos de proteção de rede devem possuir suporte a Jumbo Frames;

6.17 Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet lógicas;

6.18 Deve suportar NAT dinâmico (Many-to-1);

6.19 Deve suportar NAT dinâmico (Many-to-Many);

6.20 Deve suportar NAT estático (1-to-1);

6.21 Deve suportar NAT estático (Many-to-Many);

6.22 Deve suportar NAT estático bidirecional 1-to-1;

6.23 Deve suportar Tradução de porta (PAT);

6.24 Deve suportar NAT de Origem;

- 6.25 Deve suportar NAT de Destino;
- 6.26 Deve suportar NAT de Origem e NAT de Destino simultaneamente;
- 6.27 Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
- 6.28 Deve suportar NAT64 e NAT46;
- 6.29 Deve implementar o protocolo ECMP;
- 6.30 Deve implementar balanceamento de link por hash do IP de origem;
- 6.31 Deve implementar balanceamento de link por hash do IP de origem e destino;
- 6.32 Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, quatro links;
- 6.33 Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais;
- 6.34 Deve permitir monitorar via SNMP falhas de hardware, uso de recursos por número elevado de sessões, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster, ataques e estatísticas de uso das interfaces de rede;
- 6.35 Enviar log para sistemas de monitoração externos, simultaneamente;
- 6.36 Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;
- 6.37 Proteção anti-spoofing;
- 6.38 Implementar otimização do tráfego entre dois equipamentos;
- 6.39 Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
- 6.40 Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);

- 6.41 Suportar OSPF graceful restart;
- 6.42 Os dispositivos de proteção devem ter a capacidade de operar de forma simultânea em uma única instância de firewall, mediante o uso de suas interfaces físicas nos seguintes modos: Modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3);
- 6.43 Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
- 6.44 Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;
- 6.45 Deve suportar 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;
- 6.46 Deve suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;
- 6.47 Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em modo transparente;
- 6.48 Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3;
- 6.49 Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3 e com no mínimo 3 equipamentos no cluster;
- 6.50 A configuração em alta disponibilidade deve sincronizar: Sessões;
- 6.51 A configuração em alta disponibilidade deve sincronizar: Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede;
- 6.52 A configuração em alta disponibilidade deve sincronizar: Associações de Segurança das VPNs;
- 6.53 A configuração em alta disponibilidade deve sincronizar: Tabelas FIB;
- 6.54 O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link;

- 6.55 Deve possuir suporte a criação de sistemas virtuais no mesmo appliance;
- 6.56 A utilização dos dispositivos em alta disponibilidade não deve impor limitações quanto à utilização de sistemas virtuais (contextos);
- 6.57 Deve permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados por equipes distintas;
- 6.58 O gerenciamento da solução deve suportar acesso via SSH e interface WEB (HTTPS), incluindo, mas não limitado à, exportar configuração dos sistemas virtuais (contextos) por ambas interfaces;
- 6.59 Controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound), sendo que deve suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos);
- 6.60 As funcionalidades de controle de aplicações, VPN IPSec e SSL, QOS, SSL e SSH Decryption e protocolos de roteamento dinâmico devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante;
- 6.61 As funcionalidades de controle de aplicações, VPN IPSec e SSL, QOS, SSL e SSH Decryption e protocolos de roteamento dinâmico devem operar em caráter permanente, o licenciamento do dispositivo de segurança não pode ter nenhuma relação com sua configuração de rede como, mas não limitado a, configuração de interfaces, endereços lógicos, etc , podendo ser utilizado por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante;

Controle de Políticas de Firewall

- 6.62 Deverá suportar controles por zona de segurança;
- 6.63 Controles de políticas por porta e protocolo;
- 6.64 Controle de políticas por aplicações grupos estáticos de aplicações, grupos dinâmicos de

aplicações (baseados em características e comportamento das aplicações) e categorias de

aplicações;

- 6.65 Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;
- 6.66 Controle de políticas por código de País (Por exemplo: BR, USA, UK, RUS);
- 6.67 Controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound);
- 6.68 Deve suportar offload de certificado em inspeção de conexões SSL de entrada (Inbound);
- 6.69 Deve de-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.2;
- 6.70 Controle de inspeção e de-criptografia de SSH por política;
- 6.71 Bloqueios dos seguintes tipos de arquivos: bat, cab, dll, exe, bin, zip, tar e mp3;
- 6.72 Traffic shaping QoS baseado em Políticas (Prioridade, Garantia e Máximo);
- 6.73 QoS baseado em políticas para marcação de pacotes (diffserv marking), inclusive por aplicações;
- 6.74 Suporte a objetos e regras IPV6;
- 6.75 Suporte a objetos e regras multicast;
- 6.76 Deve suportar no mínimo três tipos de negação de tráfego nas políticas de firewall: Drop sem notificação do bloqueio ao usuário, Drop com notificação do bloqueio ao usuário, Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego, TCP-Reset para o client, TCP-Reset para o server ou para os dois lados da conexão;
- 6.77 Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;

Controle de Aplicações

- 6.78 Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer

aplicações, independente de porta e protocolo, com as seguintes funcionalidades:

- 6.79 Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;
- 6.80 Reconhecer pelo menos 1700 aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;
- 6.81 Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs, etc;
- 6.82 Deve inspecionar o payload de pacote de dados com o objetivo de detectar através de expressões regulares assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;
- 6.83 Deve detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a Encrypted Bittorrent e aplicações VOIP que utilizam criptografia proprietária;
- 6.84 Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;
- 6.85 Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
- 6.86 Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado a Yahoo Instant Messenger usando HTTP. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivo dentro do Webex;
- 6.87 Identificar o uso de táticas evasivas via comunicações criptografadas;
- 6.88 Atualizar a base de assinaturas de aplicações automaticamente;

- 6.89 Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos do LDAP/AD;
- 6.90 Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;
- 6.91 Deve ser possível adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;
- 6.92 Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;
- 6.93 Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;
- 6.94 Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão;
- 6.95 A criação de assinaturas personalizadas deve permitir o uso de expressões regulares, contexto (sessões ou transações), usando posição no payload dos pacotes TCP e UDP e usando decoders de pelo menos os seguintes protocolos: HTTP, FTP, NBSS, DCE RPC, SMTP, Telnet, SSH, MS-SQL, IMAP, DNS, LDAP, RTSP e SSL;
- 6.96 O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
- 6.97 Deve alertar o usuário quando uma aplicação for bloqueada;
- 6.98 Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;
- 6.99 Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, neonet, etc) possuindo granularidade de controle/políticas para os mesmos;
- 6.100 Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts,

Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;

6.101 Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo

permitir o Hangouts chat e bloquear a chamada de vídeo;

6.102 Deve possibilitar a diferenciação de aplicações Proxies (psiphon3, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;

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

6.104 Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como: Tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc);

6.105 Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como: Nível de risco da aplicação;

6.106 Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como: Categoria da aplicação;

6.107 Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como: Aplicações que usem técnicas evasivas, utilizadas por malwares como uso excessivo de banda, tunelamento de tráfego ou transferência de arquivos, etc;

Prevenção de Ameaças

6.108 Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de Firewall ou entregue através de composição com outro equipamento ou fabricante;

6.109 Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);

6.110 As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o

direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante;

- 6.111 Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;
- 6.112 Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS, Antipyyware e Antivirus: permitir, permitir e gerar log, bloquear, bloquear IP do atacante por um intervalo de tempo e enviar tcp-reset;
- 6.113 As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;
- 6.114 Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;
- 6.115 Exceções por IP de origem ou de destino devem ser possíveis nas regras e assinatura a assinatura;
- 6.116 Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
- 6.117 Deve permitir o bloqueio de vulnerabilidades;
- 6.118 Deve permitir o bloqueio de exploits conhecidos;
- 6.119 Deve incluir proteção contra ataques de negação de serviços;
- 6.120 Deverá possuir o seguinte mecanismos de inspeção de IPS: Análise de padrões de estado de conexões;
- 6.121 Deverá possuir o seguinte mecanismos de inspeção de IPS: Análise de decodificação de protocolo;
- 6.122 Deverá possuir o seguinte mecanismo de inspeção de IPS: Análise para detecção de anomalias de protocolo;
- 6.123 Deverá possuir o seguinte mecanismo de inspeção de IPS: Análise heurística;
- 6.124 Deverá possuir o seguinte mecanismo de inspeção de IPS: IP Defragmentation;

6.125 Deverá possuir o seguinte mecanismo de inspeção de IPS: Remontagem de pacotes de TCP;

6.126 Deverá possuir o seguinte mecanismo de inspeção de IPS: Bloqueio de pacotes

malformados;

6.127 Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;

6.128 Detectar e bloquear a origem de portscans;

6.129 Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;

6.130 Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;

6.131 Possuir assinaturas para bloqueio de ataques de buffer overflow;

6.132 Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;

6.133 Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS e anti-spyware, permitindo a criação de exceções com granularidade nas configurações;

6.134 Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;

6.135 Suportar bloqueio de arquivos por tipo;

6.136 Identificar e bloquear comunicação com botnets;

6.137 Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;

6.138 Deve suportar a captura de pacotes (PCAP), por assinatura de IPS e controle de aplicação;

6.139 Deve permitir que na captura de pacotes por assinaturas de IPS seja definido o número de

pacotes a serem capturados ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos;

6.140 Deve possuir a função de proteção a resolução de endereços via DNS, identificando

requisições de resolução de nome para domínios maliciosos de botnets conhecidas;

6.141 Os eventos devem identificar o país de onde partiu a ameaça;

6.142 Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;

6.143 Proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;

6.144 Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança;

Filtro de URL

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

6.146 Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;

6.147 Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local;

6.148 Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local, em modo de proxy transparente e explícito;

6.149 Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de

URL;

6.150 Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;

6.151 Possuir pelo menos 60 categorias de URLs;

6.152 Deve possuir a função de exclusão de URLs do bloqueio, por categoria;

6.153 Permitir a customização de página de bloqueio;

6.154 Permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão Continuar para permitir o usuário continuar acessando o site);

Identificação de Usuários

6.155 Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-directory e base de dados local;

6.156 Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

6.157 Deve possuir integração e suporte a Microsoft Active Directory para os seguintes sistemas operacionais: Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 e Windows Server 2012 R2;

6.158 Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on, essa funcionalidade não deve possuir limites licenciados de usuários ou qualquer tipo de restrição de uso como, mas não limitado à, utilização de sistemas virtuais, segmentos de rede, etc;

6.159 Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

- 6.160 Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;
- 6.161 Deve 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);
- 6.162 Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
- 6.163 Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;
- 6.164 Permitir integração com tokens para autenticação dos usuários, incluindo, mas não limitado a acesso a internet e gerenciamento da solução;
- 6.165 Prover no mínimo um token nativamente, possibilitando autenticação de duplo fator;

QoS e Traffic Shaping

- 6.166 Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, ustream, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming;
- 6.167 Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem;
- 6.168 Suportar a criação de políticas de QoS e Traffic Shaping por endereço de destino;
- 6.169 Suportar a criação de políticas de QoS e Traffic Shaping por usuário e grupo do LDAP/AD;
- 6.170 Suportar a criação de políticas de QoS e Traffic Shaping por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;
- 6.171 Suportar a criação de políticas de QoS e Traffic Shaping por porta;
- 6.172 O QoS deve possibilitar a definição de classes por Banda Garantida;

- 6.173 O QoS deve possibilitar a definição de classes por Banda Máxima;
- 6.174 O QoS deve possibilitar a definição de classes por Fila de Prioridade;
- 6.175 Suportar priorização em tempo real de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype;
- 6.176 Suportar marcação de pacotes Diffserv, inclusive por aplicação;
- 6.177 Suportar modificação de valores DSCP para o Diffserv;
- 6.178 Suportar priorização de tráfego usando informação de Type of Service;
- 6.179 Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping;
- 6.180 Deve suportar QOS (traffic-shapping), em interface agregadas ou redundantes;

Filtro de Dados

- 6.181 Permitir a criação de filtros para arquivos e dados pré-definidos;
- 6.182 Os arquivos devem ser identificados por extensão e assinaturas;
- 6.183 Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP, etc);
- 6.184 Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
- 6.185 Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
- 6.186 Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular;

Geo Localização

- 6.187 Suportar a criação de políticas por geo-localização, permitindo o tráfego de determinado

Pais/Países sejam bloqueados;

- 6.188 Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;
- 6.189 Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas;

VPN

- 6.190 Suportar VPN Site-to-Site e Cliente-To-Site;
- 6.191 Suportar IPSec VPN;
- 6.192 Suportar SSL VPN;
- 6.193 A VPN IPSEC deve suportar 3DES;
- 6.194 A VPN IPSEC deve suportar Autenticação MD5 e SHA-1;
- 6.195 A VPN IPSEC deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;
- 6.196 A VPN IPSEC deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);
- 6.197 A VPN IPSEC deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);
- 6.198 A VPN IPSEC deve suportar Autenticação via certificado IKE PKI
- 6.199 Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;
- 6.200 Suportar VPN em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPSec IPv6;
- 6.201 Deve permitir habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSec a partir da interface gráfica da solução, facilitando o processo de troubleshooting;
- 6.202 A VPN SSL deve suportar o usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;
- 6.203 A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;
- 6.204 Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro

- do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;
- 6.205 Atribuição de DNS nos clientes remotos de VPN;
- 6.206 Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
- 6.207 Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local;
- 6.208 Suportar leitura e verificação de CRL (certificate revocation list);
- 6.209 Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;
- 6.210 O agente de VPN a ser instalado nos equipamentos desktop e laptops, dever ser capaz de ser distribuído de maneira automática via Microsoft SCCM, Active Directory e ser descarregado diretamente desde o seu próprio portal, o qual residirá no centralizador de VPN;
- 6.211 Deve permitir que a conexão com a VPN seja estabelecida das seguintes forma: Antes do usuário autenticar na estação;
- 6.212 Deve permitir que a conexão com a VPN seja estabelecida das seguintes forma: Após autenticação do usuário na estação;
- 6.213 Deve permitir que a conexão com a VPN seja estabelecida das seguintes forma: Sob demanda do usuário;
- 6.214 Deverá manter uma conexão segura com o portal durante a sessão;
- 6.215 O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows XP (32 bit), Windows 7 (32 e 64 bit), Windows 8 (32 e 64 bit), Windows 10 (32 e 64 bit) e Mac OS X (v10.10 ou superior);

SERVIÇO DE PROTEÇÃO CONTRA ATAQUES DE NEGAÇÃO DE SERVIÇO DDOS

1. ESPECIFICAÇÕES GERAIS DO SERVIÇO

- 1.1 A CONTRATADA deverá prover o serviço de mitigação de ataques de negação de serviço (DoS – Denial of Service) para o circuito de conectividade IP dedicada à Internet, sejam eles distribuídos (DDoS – Distributed Denial of Service) ou não.
- 1.2 A solução deverá ser baseada no monitoramento não intrusivo do tráfego e a mitigação deve ser no backbone do fornecedor.
- 1.3 O ataque deve ser mitigado na estrutura da CONTRATADA, separando o tráfego legítimo do malicioso, de modo que os serviços de Internet da Prefeitura Municipal de São Lourenço continuem disponíveis aos seus usuários.
- 1.4 A proteção deverá operar sem exigir o desligamento de qualquer outro circuito de acesso da Prefeitura Municipal de São Lourenço, independente de quantos ou quais sejam os demais fornecedores.
- 1.5 A solução ofertada não poderá afetar a visibilidade do endereço de origem das requisições, mantendo o tráfego legítimo livre de qualquer modificação.
- 1.6 O serviço deve ser capaz de prover proteção, no mínimo, contra ataques que explorem a capacidade dos canais de comunicação (ataques volumétricos, como ICMP Flood e UDP Flood), a capacidade de processamento de requisições da infraestrutura de redes (como SYN Flood e TCP Flag Abuses) ou a capacidade de processamento dos servidores de aplicação (como GET/POST Floods e DNS Reflection Attacks).
- 1.7 A solução deve permitir a proteção, no mínimo, do tráfego dos serviços web (HTTP/HTTPS), DNS, VPN, FTP e correio eletrônico.
- 1.8 O serviço deve suportar a mitigação de ataques que utilizam técnicas de spoofing utilizando algoritmos de desafio-resposta, como SYN Cookies e TCP SYN authentication.
- 1.9 A solução deve possuir mecanismos para filtragem de pacotes anômalos, garantindo a validade das conexões, sem efetuar qualquer limitação com base no número de sessões ou de pacotes por endereço, de modo a evitar o bloqueio de usuários legítimos.
- 1.10 A CONTRATADA deverá manter uma lista dinâmica dos endereços bloqueados, retirando aqueles que deixarem de enviar requisições maliciosas após um intervalo de tempo considerado seguro.
- 1.11 O serviço deve ter capacidade de entrega de tráfego legítimo compatível com a capacidade total do circuito de acesso.
- 1.12 É exigido que a contratada possua ao menos três centros de mitigação em dois continentes distintos que atuem de forma contingenciada entre eles.
- 1.13 É exigido que a contratada possua centros de mitigação certificados ISO/IEC 27001 de 2013 que regulamenta os requisitos de técnicas de segurança em tecnologia da informação.
- 1.14 O sistema de limpeza de dados do fornecedor deve ter a capacidade global de mitigação mínima de 80 Gbps.

2. CAPACIDADE DE MITIGAÇÃO CONTRATADA

- 2.1 A capacidade dos serviços de proteção deve ser compatível com a capacidade total do circuito de acesso.
- 2.2 Considerar os seguintes níveis de atendimento da contratação de mitigação conforme tabela abaixo:

Capacidade Máxima por Ataque:	Quantidade Máxima de IP's Monitorados:
0,5 Gbps	64 IP's

3. DISPOSIÇÕES GERAIS

3.1 Em virtude do serviço IP Internet ser fornecido por empresas que detêm concessão para a prestação de Serviços de Telecomunicações, e o serviço de segurança anti-DDOS não ser considerado um serviço de telecomunicações, existe um impedimento legal à prestação de Serviços de Valor Adicionado (SVA) e outros serviços como proteção Anti-DDOS que não sejam de telecomunicações, decorrente da Lei 9472/1997, a Lei Geral de Telecomunicações (LGT). Assim sendo, é permitido consórcio entre empresas do mesmo grupo visando aumento da competitividade com vistas a atingir maior economicidade ao órgão.

Item 3

1.1 Serviço de Cloud

O de Cloud é concebido de forma a disponibilizar a infraestrutura contratada de forma ágil e flexível.

Uma Máquina Virtual construída deverá ser entregue em 15 dias úteis. As solicitações de alterações de componentes de serviços serão realizadas em 7 dias úteis, a partir da data de validação do Termo de Adesão assinado pela CONTRATANTE, desde que as características migrem para uma das características existentes no Catálogo de Serviços da CONTRATADA.

1.2 Suporte e atendimento ao serviço de Cloud

Para suporte à operação da CONTRATADA, o serviço de Cloud deverá ter à disposição um serviço 0800 para abertura de IMAC, ou seja, a CONTRATANTE poderá abrir e acompanhar chamados técnicos para requisição de serviços e incidentes.

Adicionalmente o Cloud deverá disponibilizar à CONTRATADA portais online para execução de ações de administração e operação de seu ambiente, através de acesso via URLs padronizadas a partir de seu próprio navegador Internet.

Através dos portais o usuário poderá executar várias funções de administração e operação do seu ambiente Cloud, tais como:

Administração de VMs , Visualização de LOGs e Administração de Pool de Recursos.

Algumas funções de administração / operação do ambiente Cloud que a CONTRATANTE deverá utilizar:

Reboot – Reinicializa uma VM

Shutdown – Desativa uma VM

Power Off – Desliga uma VM

Edit – Inserir informações a respeito de sua Máquina Virtual

Change Lease – Informa dados de expiração de maquinas virtuais

Destroy – Desconfigura uma maquina virtual

Expire – Expira uma VM

Outras funções aplicadas exclusivamente no ambiente da CONTRATANTE. Ex: alterações de regras de FireWall, atribuição de IPs Públicos, Suspend, etc

Independente dos portais estarem disponíveis, a CONTRATANTE poderá entrar em contato através do Serviço de Atendimento 0800 para fazer requisições de serviços (IMACs) ou abrir/acompanhar incidentes.

2 Modalidades do Serviço

Arquitetura

O Cloud é um serviço de TI cuja infraestrutura deverá estar dentro de um Data Center, com certificação TIER III. Para a CONTRATADA acessar à sua Máquina Virtual, ela deverá ter um acesso através da internet ou através de redes dedicadas. O acesso do ambiente da CONTRATADA até a internet não faz parte do escopo deste projeto e a contratação deste, é de responsabilidade da CONTRATANTE.

A solução do Cloud deve ser construída de forma a garantir a alta disponibilidade e a robustez da solução: a redundância de infraestrutura é feita está em nível de *software* como em nível de *hardware*. A rede interna do Cloud deve ser construída de forma redundante e com enlaces de alta capacidade, ou seja, a falha de um link ou um equipamento é absorvida pelo recurso redundante sem impacto no serviço final. A tecnologia de virtualização permite que, em caso de falha, uma Máquina Virtual seja transferida para outro *hardware*, sem parada de serviço.

2.1 Componentes Básicos do serviço de Cloud

2.1.1 Componentes de serviços de computação: Processamento e Memória

O conjunto de processamento e memória deverá estar agrupado logicamente em uma Máquina Virtual (VM – *Virtual Machine*) e caracterizam a capacidade computacional contratada.

Esses processadores poderão ser fisicamente compartilhados entre os clientes, mas a tecnologia de virtualização deve garantir o isolamento das informações entre as VMs assim como a garantia dos recursos contratados.

Na realização de upgrade de memória e vCPU não deverá se fazer necessária pausa do servidor FÍSICO.

Para todas as VM's nas configurações deverão ser inclusas regras básicas de firewall, sistema de antivírus, espaço em storage de 100 GB sendo 50 GB para a instalação do sistema operacional (Windows).

2.1.2 Componentes de serviços de armazenamento (Storage)

A solução deverá apresentar storage Entry Level – este disco apresenta rotação de 7500rpm com uma taxa interna de transferência de aproximadamente 150MB/s. A latência rotacional média oferecida pelo disco é de 8ms.

COMPONENTES DE SERVIÇOS DE BACKUP

Da mesma forma que o Armazenamento de Dados (Storage), o Catálogo de Serviços apresentará modalidades de configurações para os Serviços de Backup. Essas modalidades foram feitas para atender a distintas aplicações de mercado e têm diferentes características. Em relação à quantidade de backup de dados, o volume é fixo, de acordo com o contratado, e as alterações serão realizadas através de pedidos de ampliação através dos Gerentes de Negócios.

A CONTRATADA terá 5 dias úteis para disponibilizar a nova configuração a partir da data de assinatura do contrato.

A modalidade de serviço de backup:

- **Diário Full** – Nesta modalidade de backup, o cliente terá o *backup* diário. A CONTRATANTE perderá os dados entre o último backup ocorrido até a solicitação da recuperação.

O *backup* é realizado em um ambiente que a CONTRATADA não tem controle, por isso existem casos que podem ocorrer que algumas informações não estejam no *backup*. Abaixo estão alguns casos:

- As informações que estão na memória RAM da VM no momento da execução do *backup* que não estarão dentro do arquivo de recuperação ou procedimentos específicos que serão de responsabilidade do cliente. Por exemplo, às 13h00min inicia o

procedimento de *backup* do cliente que tem uma aplicação de *e-commerce*. Se existe uma transação de compra às 13h00min na memória RAM do cliente, essas informações não serão recuperadas no caso de solicitação de restauração do *backup*.

- No caso de clientes com banco de dados, o cliente será responsável pela execução dos procedimentos de *backup* de sua base de dados para garantir a integridade dos dados. Um exemplo que pode ser sugerido ao cliente é que ele faça a criação de um arquivo de *backup* de sua base de dados utilizando todos os procedimentos requeridos por um banco de dados. Este arquivo será considerado um arquivo convencional e no momento da restauração do *backup*, o cliente utilizará este arquivo para recuperação do banco de dados.

Será oferecida retenção de 15 dias, ou seja, o cliente poderá recuperar os dados de até 15 dias anteriores à solicitação.

2.1.3 Componentes de serviços de Internet

O Data Center deverá possuir uma estrutura de rede de alta capacidade para oferecer conectividade internet às VM do Cloud.

2.1.4 Componentes de serviços de Segurança

Firewall

Firewall Compartilhado

Obrigatoriamente, a CONTRATADA deverá ter um serviço de firewall compartilhado com regras padrões para todos os clientes do Cloud . Para garantir que o tráfego dos clientes não se misture, o tráfego da VM deverá ser encapsulado em VLAN exclusivas para cada cliente . Isso garantirá o isolamento do tráfego de cada cliente do Cloud.

VPN IPSec

O CONTRATADA poderá acessar sua Máquina Virtual de forma remota através da internet de forma aberta e sem autenticação ou através de uma VPN IPSec que garante maior segurança e criptografia dos dados.

O tipo de conectividade deverá ser do tipo host-to-site, isto é, a CONTRATADA poderá iniciar a VPN do computador que ele queira acessar a VM e fechá-la na rede do Data Center que é um ambiente seguro e confiável.

2.1.5 Componentes de Serviços de Reconfiguração/IMAC

A CONTRATADA deverá ter direito a personalização/configurações através de chamadas por telefone (IMACs) feitos através de contato com o Data Center através de um serviço de 0800.

2.1.6 componentes de Serviços de IP público

O serviço de Cloud deverá oferecer a opção de contratação e configuração de IP Público para a Máquina Virtual desejada pela CONTRATADA.

3 Escopo de Fornecimento – Cloud

3.1 Solução Técnica

Características resumidas da solução se encontra na tabela abaixo:

VM	COMPOSIÇÃO VM	QTDE
VM 4	4 vCPU, 8 GB RAM, (Antivirus, Firewall Padrão)	1
ATRIBUTOS ADICIONAIS	DESCRIÇÃO DETALHADA	
STORAGE	1 TB	1
SISTEMA OPERACIONAL	Windows Server Data Center 2012	1
IP Público	IP Público, por VM	1
BANDA INTERNET	Banda Internet (10 Mbps)	1
CONTEXTO SDN	VPN IP SEC +Contexto de firewall + balanceamento	1
Relatórios	Utilização do link e recursos CPU e Memória	1
INSTALAÇÃO	INSTALAÇÃO ADESÃO/ALTERAÇÃO	
Adesão mensalizado 12 meses	Instalação adesão mensalizado 12 meses por contrato	1

4 Condições de prestação do serviço

4.1.1 Fluxo de Atendimento

As requisições de serviços e comunicação de incidentes deverão ser feitas para a Central de Relacionamento via 0800. O atendimento deverá ser realizado 24 horas por dia, 7 dias por semana, 365 dias por ano.

A CONTRATANTE deverá designar profissionais da área de infraestrutura e Sistemas, como contatos autorizados junto a Central de Relacionamento. Os nomes deverão ser definidos durante o processo de implantação do serviço e poderão ser atualizados posteriormente por meio de uma requisição de serviço.

A Central de Relacionamentos deverá efetuar o acompanhamento das solicitações e das soluções dadas a CONTRATANTE. A cada solicitação deverá ser associado um número de registro (chamado).

O chamado somente será concluído com o "de acordo" dado por um dos contatos autorizados. O contato será feito por telefone ou e-mail.

A CONTRATADA deverá disponibilizar 03 (três) níveis de suporte para atendimento a CONTRATANTE:

- Suporte 1º nível: Realizado pelas equipes de Service Desk e de Operação que trabalham 24x7 para atendimento a qualquer nível de severidade de problemas.
- Suporte 2º nível: Realizado pela equipe de Suporte que trabalha on site, para atendimento de chamados de todas as severidades.
- Suporte 3º nível: Realizado pela equipe de especialistas que trabalham on site e são acionados para atendimento dos chamados não solucionados pelo suporte de 2º nível.

Em caso de incidentes de alta criticidade, o chamado é enviado simultaneamente para todas as equipes de suporte.

4.1.2 Acordos de Nível de Serviço

CENTRAL DE SERVIÇOS

A Central de Serviços deverá possuir de Acordos de Nível de Serviço (SLA – Service Level Agreements) baseados em tempo de início de atendimento, diagnóstico e notificação a CONTRATANTE.

Tempo de Atendimento de ocorrências

É o tempo que a monitoração terá para realizar a validação de um incidente ou evento detectado pelas ferramentas de gerenciamento e a respectiva confirmação para a abertura do chamado no Sistema de Registro de Chamados, somado ao tempo que o Service Desk terá para notificação da ocorrência a CONTRATANTE.

Em caso de notificação de ocorrência realizada pela CONTRATANTE o tempo que o Service Desk deverá ter para o atendimento será aquele transcorrido entre a comunicação feita pela

CONTRATANTE, o registro na ferramenta e o devido retorno do número da ocorrência.

- Severidade 1: 15 min
- Severidade 2: 30 min
- Severidade 3: 2 horas
- Severidade 4: 4 horas

Tempo de Diagnóstico e Notificação

Entende-se por diagnóstico a descrição sobre o entendimento do evento com a indicação da solução de contorno ou definitiva.

Notificação é uma atualização da ocorrência e a devida informação a CONTRATANTE.

Tempo de diagnóstico é o tempo que o fornecedor terá para realizar e registrar o primeiro diagnóstico, seja uma ocorrência ou uma solicitação, contado desde a abertura do chamado e de acordo com a severidade definida.

A primeira notificação deve ocorrer no tempo indicado pela severidade, contado após o tempo de diagnóstico. A segunda notificação ocorrerá da mesma forma, contado após o tempo da primeira notificação.

- Severidade 1: diagnóstico em 45 min, 1ª notificação em 1 hora, 2ª notificação em 3 horas.
- Severidade 2: diagnóstico em 90 min, 1ª notificação em 4 horas, 2ª notificação em 6 horas.
- Severidade 3: diagnóstico em 4 horas, 1ª notificação em 6 horas, 2ª notificação em 10 horas.

- Severidade 4: diagnóstico em 24 h, 1ª notificação em 12 horas, 2ª notificação em 12 horas.

Outros indicadores

Item	Indicador	Nível de Serviço Aceitável	Período de Apuração
1	Taxa de Abandono	<= 5% das ligações abandonadas após espera superior a 10 segundos	Mensal
2	Taxa de Solução em Primeiro Contato (FCR)	> 70% de chamados solucionados pelo 1º Nível em primeiro contato para "Ilha Técnica"	Mensal
3	Atendimento 1º Nível em até 10 segundos	>= 95% dos chamados atendidos pelo 1º Nível em até 10 segundos	Mensal
4	Tempo de resposta de atendimentos via e-mail	> 95% dos e-mail atendidos em até 30 minutos	Mensal

Descrição dos níveis de Severidade

- Severidade 1

Serviço seriamente afetado e indisponível para muitos usuários.

Não existe alternativa disponível para que os usuários possam trabalhar.

A parada do serviço pode resultar em perda de receita da CONTRATANTE.

A porcentagem de incidências neste nível não deve exceder 25% do total de incidências registradas por mês.

- Severidade 2

Serviço afetado para muitos usuários ou indisponível para um usuário.

Não existe alternativa disponível para que os usuários possam trabalhar.

A parada do serviço pode resultar em perda de produtividade, colocando em risco benefícios ou receita da CONTRATANTE.

- Severidade 3

Serviço afetando um usuário.

Existem alternativas disponíveis para que o usuário possa trabalhar, porém outras atividades podem ser afetadas enquanto se espera a resolução do problema.

A interrupção do serviço pode causar redução de produtividade, porém não afeta ingressos de recursos financeiros.

- Severidade 4

O serviço a um usuário individual está afetado resultando em um inconveniente.

Existem alternativas disponíveis para executar o trabalho.

A interrupção do serviço não resulta em impacto imediato ao negócio.

4.1.3 INFRAESTRUTURA DE DATA CENTER

Esses acordos de nível de serviço representam os parâmetros de qualidade do serviço, no que tange a disponibilidade de infraestrutura do Data Center.

O SLA mensal de disponibilidade de Infraestrutura indica qual a porcentagem de tempo que a infraestrutura deverá estar disponível em relação ao tempo total medido no mês.

O tempo de disponibilidade da infraestrutura é a diferença entre o tempo total medido no mês e o tempo de indisponibilidade, por motivos não planejados, da infraestrutura.

Os padrões de qualidade de serviço para o presente escopo são os definidos a seguir.

Infraestrutura de energia elétrica

- Data Center (certificado Tier III) – 99,98%

Infraestrutura de refrigeração

- Data Center (certificado Tier III) – 99,98%

Infraestrutura de Backbone (rede interna de dados) do Data Center

- Data Center (certificado Tier III) – 99,95%

Cálculo dos índices de disponibilidade de Infraestrutura

O cálculo dos índices de disponibilidade acima estabelecidos será efetuado aplicando-se a fórmula abaixo:

$$ID = \{[(DR + IJ) / DP] \times 100\}$$

Onde: ID = Índice de disponibilidade

DR = Disponibilidade real no mês

IJ = Indisponibilidade justificada no mês

DP = Disponibilidade prevista = número de dias do mês x 24h

Nota: A indisponibilidade justificada decorre de:

- Períodos de manutenção;
- Paradas acordadas;
- Motivos de força maior (guerras, terremotos, enchentes, etc.).

Ressarcimento por indisponibilidade de infraestrutura

O valor a ser ressarcido por indisponibilidade de infraestrutura é determinado de acordo com a tabela de descontos a seguir, sendo o percentual estabelecido aplicado sobre o valor mensal contratado.

Diferenças (%)	Descontos (%)
$0 < DC \leq 2$	5
$2 < DC \leq 4$	7,5
$4 < DC \leq 6$	10
$6 < DC \leq 8$	12,5
$8 < DC \leq 10$	15
$DC > 10$	20

$DC = SLA - ID$

Onde: DC = Desconto Calculado / SLA = % Compromissado / ID = Índice de Disponibilidade

A disponibilidade que garante o serviço obedece às seguintes condições:

- não serão contabilizadas as interrupções motivadas pela CONTRATANTE.

- no caso de necessidade de acesso da CONTRATADA as dependências da CONTRATANTE para resolução do incidente, não será considerado para o cálculo de desconto de indisponibilidade o período necessário para liberação /autorização da entrada do técnico.
- Periodicamente podem ser necessárias paradas técnicas com o objetivo de executar reconfigurações, atividades de manutenção, etc. Tais atividades, desde que programadas e comunicadas previamente a CONTRATANTE não serão contabilizadas para o cálculo da disponibilidade do serviço.

QUANTIDADES

A-SERVIÇOS DE TELEFONIA FIXA- DIGITAL (DDR)

Subitem	DESCRIÇÃO DOS SERVIÇOS	QUANT
1.1	Assinatura – Acesso digital (endereços a definir)	2
1.2	Ramais	160
1.3	Fixo - fixo local + conexão (em minutos)	16.000
1.4	Longa Distancia fixo – fixo – Intra (em minutos)	1.900
1.5	Longa Distancia fixo – fixo – Inter (em minutos)	150
1.6	Fixo - móvel local - (VC1) (em minutos)	3.000
1.7	Longa distancia Fixo - móvel VC2 (em minutos)	100
1.8	Longa distancia Fixo - móvel VC3 (em minutos)	50

B- SERVIÇOS DE TELEFONIA FIXA - SERVIÇOS ESPECIAIS VINCULADOS AOS ACESSOS DIGITAIS ou ANALOGICOS

Subitem	DESCRIÇÃO DOS SERVIÇOS	QUANT
1.1	Assinatura- 0800 ABRANGENCIA LOCAL	2
1.2	Fixo- Fixo Local (0800) (em minutos)	42
1.2.1	Movel- Fixo Local (0800) VC1 (em minutos)	280
1.3	Fixo-fixo 151,153,156,192,199 (acessos)	5
1.4	Assinatura Código especial 151,153,156,192,199	5

C- SERVIÇOS DE TELEFONIA FIXA - LINHAS ANALÓGICAS

Subitem	DESCRIÇÃO DOS SERVIÇOS	QUANT
1.1	Assinatura – Linhas analógicas (Endereços a definir pela contratante)	86
1.2	Fixo - fixo local + conexão (em minutos)	17.000
1.3	Longa Distancia fixo – fixo – Intra (em minutos)	2.000
1.4	Longa Distancia fixo – fixo – Inter (em minutos)	120
1.5	Fixo - móvel local - (VC1) (em minutos)	6.900
1.6	Longa distancia Fixo - móvel VC2 (em minutos)	200
1.7	Longa distancia Fixo - móvel VC3 (em minutos)	50

D- SERVIÇOS DE BANDA LARGA - VINCULADOS AS LINHAS ANALÓGICAS

Subitem	DESCRIÇÃO DOS SERVIÇOS	QUANT
1.1	Banda Larga – 02 mega ou menor	30
1.2	Banda Larga – 04 mega	8
1.3	Banda Larga – 08 ou 10 mega	12
1.4	Banda Larga – 15 mega ou acima	6

E-ACESSOS IP DEDICADO EM FIBRA FIM A FIM

Subitem	DESCRIÇÃO DOS SERVIÇOS	QUANT
1.1	ACESSO IP DEDICADO 80 MEGA – Paço -Rua 1 A, 332 Centro	1
1.2	ACESSO IP DEDICADO 20 MEGA – Paço -Rua 1 A, 332 Centro	1

F-MSS E DATACENTER

Subitem	DESCRIÇÃO DOS SERVIÇOS	QUANT
1.1	SERVIÇO DE SEGURANÇA GRENCIADA (MSS)	1
1.2	PROTEÇÃO CONTRA ATAQUES DE NEGAÇÃO DE SERVIÇO (ADDOS)	1
2.1	SERVIÇOS DE DATACENTER - SERVIDOR VIRTUAL	1

Santa Gertrudes/SP, 11 de julho de 2018.

Rogério Pascon
Prefeito Municipal

PREGAO PRESENCIAL 19/2018

ANEXO II – FORMULÁRIO DE PROPOSTA FINANCEIRA

A-SERVIÇOS DE TELEFONIA FIXA- DIGITAL (DDR):

Subitem	DESCRIÇÃO DOS SERVIÇOS	QUANT	VL UNITARIO	VL MENSAL
1.1	Assinatura – Acesso digital (endereços a definir)	2		
1.2	Ramais	160		
1.3	Fixo - fixo local + conexão (em minutos)	16.000		
1.4	Longa Distancia fixo – fixo – Intra (em minutos)	1.900		
1.5	Longa Distancia fixo – fixo – Inter (em minutos)	150		
1.6	Fixo - móvel local - (VC1) (em minutos)	3.000		
1.7	Longa distancia Fixo - móvel VC2 (em minutos)	100		
1.8	Longa distancia Fixo - móvel VC3 (em minutos)	50		

B-SERVIÇOS DE TELEFONIA FIXA - SERVIÇOS ESPECIAIS VINCULADOS AOS ACESSOS DIGITAIS ou ANALOGICOS:

Subitem	DESCRIÇÃO DOS SERVIÇOS	QUANT	VL UNITARIO	VL MENSAL
1.1	Assinatura- 0800 ABRANGENCIA LOCAL	2		
1.2	Fixo- Fixo Local (0800) (em minutos)	42		
1.2.1	Movel- Fixo Local (0800) VC1 (em minutos)	280		
1.3	Fixo-fixo 151,153,156,192,199 (acessos)	5		
1.4	Assinatura Código especial 151,153,156,192,199	5		

C-SERVIÇOS DE TELEFONIA FIXA - LINHAS ANALÓGICAS:

Subitem	DESCRIÇÃO DOS SERVIÇOS	QUANT	VL UNITARIO	VL MENSAL
1.1	Assinatura – Linhas analógicas (Endereços a definir pela contratante)	86		

1.2	Fixo - fixo local + conexão (em minutos)	17.000		
1.3	Longa Distancia fixo – fixo – Intra (em minutos)	2.000		
1.4	Longa Distancia fixo – fixo – Inter (em minutos)	120		
1.5	Fixo - móvel local - (VC1) (em minutos)	6.900		
1.6	Longa distancia Fixo - móvel VC2 (em minutos)	200		
1.7	Longa distancia Fixo - móvel VC3 (em minutos)	50		

D-SERVIÇOS DE BANDA LARGA - VINCULADOS AS LINHAS ANALÓGICAS:

Subitem	DESCRIÇÃO DOS SERVIÇOS	QUANT	VL UNITARIO	VL MENSAL
1.1	Banda Larga – 02 mega ou menor	30		
1.2	Banda Larga – 04 mega	8		
1.3	Banda Larga – 08 ou 10 mega	12		
1.4	Banda Larga – 15 mega ou acima	6		

E-ACESSOS IP DEDICADO EM FIBRA FIM A FIM:

Subitem	DESCRIÇÃO DOS SERVIÇOS	QUANT	VL UNITARIO	VL MENSAL
1.1	ACESSO IP DEDICADO 80 MEGA – Paço -Rua 1 A, 332	1		
1.2	ACESSO IP DEDICADO 20 MEGA – Paço -Rua 1 A, 332	1		

F-MSS, ADDOS E DATA CENTER:

Subitem	DESCRIÇÃO DOS SERVIÇOS	QUANT	VL UNITARIO	VL MENSAL
1.1	SERVIÇO DE SEGURANÇA GERENCIADA (MSS)	1		
1.2	PROTEÇÃO CONTRA ATAQUES DE NEGAÇÃO DE SERVIÇO (ADDOS)	1		
2.1	SERVIÇOS DE DATACENTER - SERVIDOR VIRTUAL	1		

VALOR GLOBAL (A+B+C+D+E+F) MENSAL R\$

_____ (_____)

VALOR GLOBAL (A+B+C+D+E+F) ANUAL

R\$ _____ (_____)

Preços completos, computando todos os custos necessários para o atendimento do objeto desta licitação, bem como todos os insumos, impostos, encargos trabalhistas, previdenciários, fiscais, comerciais, taxas, transportes e quaisquer outros que incidam ou venham a incidir sobre o objeto licitado, constante desta proposta.

Declaramos que os materiais ofertados por nossa empresa, atendem rigorosamente, as características necessárias arroladas no objeto da licitação.

Dados cadastrais da proponente:

Razão Social: _____

Endereço: _____

Município/UF: _____ Bairro: _____

Fone: (_____) _____ Fax: (_____) _____

CNPJ (MF): _____

Inscrição Estadual: _____

Tipo de Registro: (Registro em Cartório ou Registro na Junta Comercial ou Registro na OAB):

Número do Registro: _____

Data do Registro: _____

E-mail

INSTITUCIONAL: _____

Dados Bancários: Banco: _____; Agência: _____; Conta Corrente: _____

Validade da proposta: _____ (_____) dias corridos (mínimo 60 dias)

Condições de pagamento: Os pagamentos serão realizados mediante fatura, com data de vencimento pactuada entre as partes. As faturas deverão ser apresentadas mensalmente;

Prazo de início dos serviços: **Imediato, após a assinatura do contrato;**

Prazo para execução dos serviços: Até 60 dias a contar da assinatura do contrato, com possibilidade de prorrogação por mais 30 dias, mediante justificativa.

Indicação dos Dados **DO REPRESENTANTE LEGAL QUE ASSINARÁ O CONTRATO,**
em caso de vitória no certame:

Nome: _____

Nacionalidade: _____; Profissão: _____

Estado Civil: _____

Endereço Residencial (completo - com CEP.):

Telefone **PESSOAL:** (_____) _____;

E-mail **PESSOAL**: _____;

Data de Nascimento: ____/____/____;

RG.: _____; CPF.: _____;

Função do Responsável:

Participação do Responsável na empresa (%):

Data da inclusão do sócio na empresa:

Dados cadastrais **DE TODOS OS REPRESENTANTES LEGAIS DA EMPRESA:**

Nome:

Nacionalidade:

Estado Civil:

CPF:

RG:

Endereço:

Bairro:

Município:

Estado:

CEP:

Telefone **PESSOAL**: (____) _____;

E-mail **PESSOAL**: _____;

Data de Nascimento: ____/____/____;

Função do Responsável:

Participação do Responsável na empresa (%):

Data da inclusão do sócio na empresa:

Declaramos que assumimos a prestação dos serviços, por nossa conta e risco, ficando sob nossa inteira e exclusiva responsabilidade a prestação dos mesmos.

Local e Data: _____

Carimbo e Assinatura: _____

PREGÃO PRESENCIAL 19/2018

**ANEXO III - MODELO DE DECLARAÇÃO DE PLENO ATENDIMENTO AOS
REQUISITOS DE HABILITAÇÃO**

DECLARAÇÃO

À
Prefeitura do Município de Santa Gertrudes
Rua 01A, 332, Centro
Santa Gertrudes - SP

A empresa _____,
estabelecida na _____, Bairro _____,
_____/_____, CEP: _____, Telefone (_____) _____,
inscrita com CNPJ _____, neste ato representada pelo seu
(representante/sócio/procurador) _____, portador do RG
_____ e do CPF _____, no uso de suas atribuições
legais, vem:

Declarar, para fins de participação no processo licitatório em pauta,
sob as penas da Lei, que cumpre plenamente aos requisitos de habilitação.

Por ser verdade assina a presente.

Local e Data: _____

Razão Social da Empresa
Nome do responsável/procurador
Cargo do responsável/procurador
Documento de identidade

PREGÃO PRESENCIAL 19/2018

**ANEXO IV - MODELO DE DECLARAÇÃO DE INEXISTÊNCIA DE FATO
IMPEDITIVO**

DECLARAÇÃO

À
Prefeitura do Município de Santa Gertrudes
Rua 01A, 332, Centro
Santa Gertrudes - SP

A empresa _____,
estabelecida na _____, Bairro _____,
_____/____, CEP: _____, Telefone (____) _____,
inscrita com CNPJ _____, neste ato representada pelo seu
(representante/sócio/procurador) _____, portador do RG
_____ e do CPF _____, no uso de suas atribuições
legais, vem:

Declarar, para fins de participação no processo licitatório em pauta,
sob as penas da Lei, que não se encontra penalizada por declaração de inidoneidade ou
impedimento de licitar e contratar com quaisquer entes da Administração Pública, e que se
compromete a comunicar ocorrência de fatos supervenientes.

Por ser verdade assina a presente.

Local e Data: _____

Razão Social da Empresa

Nome do responsável/procurador
Cargo do responsável/procurador
Documento de identidade

PREGÃO PRESENCIAL 19/2018

**ANEXO V - MODELO DE DECLARAÇÃO DE REGULARIDADE PARA COM O
MINISTÉRIO DO TRABALHO**

DECLARAÇÃO

À
Prefeitura do Município de Santa Gertrudes
Rua 01A, 332, Centro
Santa Gertrudes - SP

A empresa _____,
estabelecida na _____, Bairro _____,
_____/____, CEP: _____, Telefone (____) _____,
inscrita com CNPJ _____, neste ato representada pelo seu
(representante/sócio/procurador) _____, portador do RG
_____ e do CPF _____, no uso de suas atribuições
legais, vem:

Declarar, para fins de participação no processo licitatório em pauta,
sob as penas da Lei, que está em situação regular perante o Ministério do Trabalho, no que se
refere à observância do disposto no inciso XXXIII, do artigo 7º da Constituição Federal, e, para
fins do disposto no inciso V do artigo 27 da Lei Federal 8.666/93, acrescido pela Lei 9.854, de
27 de outubro de 1999, que não emprega menor de 18 (dezoito) anos em trabalho noturno,
perigoso ou insalubre e não emprega menor de 16 (dezesseis) anos.

Ressalva: emprega menor, a partir de 14 (quatorze) anos, na condição
de aprendiz (____). Observação: em caso afirmativo, assinalar a ressalva acima.

Por ser verdade assina a presente.

Local e Data: _____

Razão Social da Empresa
Nome do responsável/procurador
Cargo do responsável/procurador
Documento de identidade

PREGÃO PRESENCIAL 19/2018

ANEXO VI – MODELO DE DECLARAÇÃO DE MICRO E PEQUENA EMPRESA

DECLARAÇÃO

À
Prefeitura do Município de Santa Gertrudes
Rua 01A, 332, Centro
Santa Gertrudes - SP

A empresa _____,
estabelecida na _____, Bairro _____,
_____/_____, CEP: _____, Telefone (_____) _____,
inscrita com CNPJ _____, neste ato representada pelo seu
(representante/sócio/procurador) _____, portador do RG
_____ e do CPF _____, no uso de suas atribuições
legais, vem

Declarar, para fins de participação no processo licitatório em pauta,
sob as penas da Lei, que é Microempresa (ME) ou Empresa de Pequeno Porte (EPP), nos termos
da Lei Complementar nº 123/06, estando apta, portanto, a exercer o direito de preferência a que
faz jus no procedimento licitatório em epígrafe, realizado pela Prefeitura Municipal De Santa
Gertrudes /SP.

Por ser verdade assina a presente.

Local e Data: _____

Razão Social da Empresa
Nome do responsável/procurador
Cargo do responsável/procurador

Documento de identidade

ESTE DOCUMENTO DEVE SER APRESENTADO A PREGOEIRA NA FASE DE
CREDENCIAMENTO FORA DOS ENVELOPES Nº 01 (PROPOSTA) E 02
(DOCUMENTAÇÃO)

PREGÃO PRESENCIAL 19/2018

**ANEXO VII – MINUTA DO CONTRATO QUE ENTRE SI CELEBRAM A
PREFEITURA DO MUNICÍPIO DE SANTA GERTRUDES E A EMPRESA
XXXXXXXXXXXXXXXXXXXX PARA A PRESTAÇÃO DE SERVIÇOS DE TELEFONIA,
INTERNET E SEGURANÇA DIGITAL**

DATA: ____ de _____ de 2018.

PRAZO: 12(doze) meses, com possibilidade de prorrogação.

VALOR GLOBAL ESTIMATIVO: R\$ _____.

LICITAÇÃO: Pregão Presencial 19/2018.

CONTRATO: __/2018.

Cláusula 1ª - DAS PARTES

1.1. A **Prefeitura do Município de Santa Gertrudes**, inscrita com CNPJ 45.732.377/0001-73, com sede à Rua 01A, 332, Centro, Santa Gertrudes/SP, E-mail: gabinete@santagertrudes.sp.gov.br, representada neste ato pelo Prefeito Municipal, **Rogério Pascon**, brasileiro, casado, empresário, residente e domiciliado à Avenida 02, nº 572, Jd. Iporanga, Santa Gertrudes/SP, CEP.: 13.510-000, portador do CPF 082.535.568-02 e do RG 18.898.286-3/SSP/SP, E-mail: rogeriopascon@hotmail.com, adiante designada simplesmente PREFEITURA, e;

1.2. A empresa _____, inscrita com CNPJ _____, com sede a Rua/Avenida _____, __, Bairro, _____/__, CEP: _____, E-mail institucional: _____, Telefone (__) _____, Dados Bancários: Banco: _____, Agência: _____, Conta Corrente: _____, E-mail **INSTITUCIONAL:** _____, diante designada simplesmente CONTRATADA, por seu representante legal, _____, nacionalidade, estado civil, portador do CPF _____ e do RG _____, residente e domiciliado a Rua/Avenida _____, __, Bairro, _____/__, CEP: _____, E-mail **PESSOAL:** _____, ajustam o seguinte:

Cláusula 2ª - DO OBJETO

2.1. A CONTRATADA obriga-se a prestar serviços à PREFEITURA, de **telefonía, internet e segurança digital, conforme especificações contidas no Anexo I (Termo de Referência) à este edital.**

2.2. Os serviços serão interrompidos se ocorrer o término das quantias estimadas pela PREFEITURA, se não houver a necessidade de sua totalidade, a critério da PREFEITURA ou até 12(doze) meses, prevalecendo o que ocorrer primeiro, podendo ser aditado em até 25% (vinte e cinco por cento) do valor inicial atualizado do contrato, conforme o disposto no § 1º, do artigo 65, da Lei Federal Nº: 8.666/93 e alterações.

Cláusula 3ª - DO PREÇO GLOBAL ESTIMADO

3.1. Pela prestação dos serviços, a PREFEITURA pagará à CONTRATADA a seguinte importância mensal:

3.1.1. SERVIÇOS DE TELEFONIA FIXA- DIGITAL (DDR):

Subitem	DESCRIÇÃO DOS SERVIÇOS	QUANT	VL UNITARIO	VL MENSAL
1.1	Assinatura – Acesso digital (endereços a definir)	2		
1.2	Ramais	160		
1.3	Fixo - fixo local + conexão (em minutos)	15.000		
1.4	Longa Distancia fixo – fixo – Intra (em minutos)	1.900		
1.5	Longa Distancia fixo – fixo – Inter (em minutos)	150		
1.6	Fixo - móvel local - (VC1) (em minutos)	3.000		
1.7	Longa distancia Fixo - móvel VC2 (em minutos)	200		
1.8	Longa distancia Fixo - móvel VC3 (em minutos)	50		

3.1.2.SERVIÇOS DE TELEFONIA FIXA - SERVIÇOS ESPECIAIS VINCULADOS AOS ACESSOS DIGITAIS ou ANALÓGICOS:

Subitem	DESCRIÇÃO DOS SERVIÇOS	QUANT	VL UNITARIO	VL MENSAL
1.1	Assinatura- 0800 ABRANGENCIA LOCAL	2		
1.2	Fixo- Fixo Local (0800) (em minutos)	42		
1.2.1	Movel- Fixo Local (0800) VC1 (em minutos)	280		
1.3	Fixo-fixo 151,153,156,192,199 (acessos)	5		
1.4	Assinatura Código especial 151,153,156,192,199	5		

3.1.3.SERVIÇOS DE TELEFONIA FIXA - LINHAS ANALÓGICAS:

Subitem	DESCRIÇÃO DOS SERVIÇOS	QUANT	VL UNITARIO	VL MENSAL
1.1	Assinatura – Linhas analógicas (Endereços a definir pela contratante)	90		
1.2	Fixo - fixo local + conexão (em minutos)	14.000		
1.3	Longa Distancia fixo – fixo – Intra (em	2.000		

	minutos)			
1.4	Longa Distancia fixo – fixo – Inter (em minutos)	200		
1.5	Fixo - móvel local - (VC1) (em minutos)	6.000		
1.6	Longa distancia Fixo - móvel VC2 (em minutos)	200		
1.7	Longa distancia Fixo - móvel VC3 (em minutos)	50		

3.1.4.SERVIÇOS DE BANDA LARGA - VINCULADOS AS LINHAS ANALÓGICAS:

Subitem	DESCRIÇÃO DOS SERVIÇOS	QUANT	VL UNITARIO	VL MENSAL
1.1	Banda Larga – 02 mega ou menor	30		
1.2	Banda Larga – 04 mega	8		
1.3	Banda Larga – 08 ou 10 mega	12		
1.4	Banda Larga – 15 mega ou acima	6		

3.1.5.ACESSOS IP DEDICADO EM FIBRA FIM A FIM:

Subitem	DESCRIÇÃO DOS SERVIÇOS	QUANT	VL UNITARIO	VL MENSAL
1.1	ACESSO IP DEDICADO 80 MEGA – Paço -Rua 1 A, 332	1		
1.2	ACESSO IP DEDICADO 20 MEGA – Paço -Rua 1 A, 332	1		

3.1.6.MSS, ADDOS E DATA CENTER:

Subitem	DESCRIÇÃO DOS SERVIÇOS	QUANT	VL UNITARIO	VL MENSAL
1.1	SERVIÇO DE SEGURANÇA GERENCIADA (MSS)	1		
1.2	PROTEÇÃO CONTRA ATAQUES DE NEGAÇÃO DE SERVIÇO (ADDOS)	1		
2.1	SERVIÇOS DE DATACENTER - SERVIDOR VIRTUAL	1		

3.2. Nos preços estão inclusas, além do lucro, as despesas de mão-de-obra, insumos, alimentos, veículos, equipamentos, carga, seguros, impostos, taxas, transportes, manutenção, despesas de escritório e expediente e quaisquer outras despesas que estejam, direta ou indiretamente, relacionadas com a execução total deste contrato.

Cláusula 4ª - DAS CONDIÇÕES DE PAGAMENTO

4.1. Os pagamentos serão realizados mediante fatura, com data de vencimento pactuada entre as partes.

4.2. A PREFEITURA, através da tesouraria, fará as retenções dos valores correspondentes às obrigações previdenciárias, tributárias e fiscais, conforme o caso, de

acordo com a legislação que disciplina a matéria, sendo que, as guias dos valores retidos serão devidamente recolhidas e encaminhadas suas cópias reprográficas a CONTRATADA.

4.3. Caso o dia de pagamento coincida com sábados, domingos, feriados ou pontos facultativos, o mesmo será efetuado no primeiro dia útil subsequente sem qualquer incidência de correção monetária ou reajuste.

4.4. No caso da PREFEITURA atrasar os pagamentos, estes serão atualizados financeiramente “pro rata dies”, pelo IGPM/FGV/SP – Índice Geral de Preços de Mercado da Fundação Getúlio Vargas de São Paulo, em vigor na data do efetivo pagamento, ou outro índice que vier a substituí-lo, critério da PREFEITURA.

4.5. A nota fiscal/fatura encaminhada pela contratada deve estar devidamente discriminada, de forma a permitir o cumprimento das exigências legais, inclusive no que se refere às retenções tributárias.

4.6. No caso de devolução da(s) nota(s) fiscal(is)/fatura(s), por sua inexatidão ou da dependência de carta corretiva, nos casos em que a legislação admitir, o prazo fixado no item 4.1 será contado da data de entrega da referida correção.

4.7. O e-mail que deve ser cadastrado para envio das notas fiscais é o nfe@santagertrudes.sp.gov.br.

Cláusula 5ª - DO PRAZO CONTRATUAL

5.1. O contrato vigorará por 12 (doze) meses, contado da data de sua celebração, podendo ser prorrogado por até **60(sessenta)** meses corridos e consecutivos, por tratar-se de serviços de natureza continuada, nos moldes do disposto no artigo 57, da Lei Federal Nº: 8.666/93 e alterações se houver interesse das partes, mediante aviso prévio escrito.

Cláusula 6ª - DAS RESPONSABILIDADES DA CONTRATADA

6.1. A CONTRATADA reconhece por este instrumento que é a única e exclusiva responsável por danos ou prejuízos que possam causar à PREFEITURA, coisas ou pessoas de terceiros, correndo às suas expensas, sem quaisquer ônus para a PREFEITURA, ressarcimento ou indenização que tais danos ou prejuízos, nos termos do Código Civil Brasileiro e legislação pertinente.

6.2. A CONTRATADA obriga-se a permitir a fiscalização municipal, possibilitando verificar a procedência e a qualidade dos serviços entregues.

6.3. A PREFEITURA, através da Secretaria de Administração e Planejamento, poderá em qualquer ocasião, exercer a mais ampla fiscalização dos serviços, reservando-se o direito de rejeitá-los a seu critério, quando não forem considerados satisfatórios, devendo a CONTRATADA refazê-los às suas expensas.

6.4. Constatadas irregularidades no objeto contratual, na forma na cláusula anterior, a PREFEITURA poderá:

6.4.1. Se disser respeito à especificação, rejeição por quaisquer dos motivos elencados na cláusula anterior, rejeitá-lo no todo ou em parte, determinando sua substituição ou rescindindo a contratação, sem prejuízo das penalidades cabíveis;

6.4.2. Na hipótese de substituição, a CONTRATADA, as suas expensas, deverá fazê-la em conformidade com a indicação do órgão requisitante, no prazo máximo de 02 (duas) horas, contados da notificação por escrito;

6.4.3. Na hipótese de complementação, a CONTRATADA deverá fazê-la em conformidade com a indicação da PREFEITURA, no prazo máximo de 02 (duas) horas, contados da notificação por escrito.

6.5. É de inteira responsabilidade da CONTRATADA, a entrega, a configuração e testes necessários ao fiel e perfeito funcionamento dos produtos e serviços licitados.

6.6. A CONTRATADA deverá manter, durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas no edital, devendo comunicar à CONTRATANTE, imediatamente, qualquer alteração que possa comprometer a manutenção ou qualidade da contratação.

6.7. A CONTRATADA deverá atender às solicitações formais de suporte e informações técnicas de utilização e manuseio dos produtos e serviços, de acordo com a necessidade dos servidores a serviço da CONTRATANTE.

6.8. Os prazos para atendimento deverão atender o descrito no Anexo I – Termo de Referência;

6.9. Todas as requisições e consultas, com exceção das que forem feitas por telefone, deverão ser formalizadas.;

6.10. Designar, por escrito, no ato de recebimento da Ordem de Serviço, presposto que tenha poder para resolução de possíveis ocorrências durante a execução deste contrato, informando, pelo menos, o nome, telefone comercial e e-mail do mesmo;

Cláusula 7ª - DAS RESPONSABILIDADES DA CONTRATANTE

7.1. Proporcionar todas as facilidades necessárias, para que a CONTRATADA possa cumprir as condições estabelecidas neste contrato;

7.2. Efetuar os pagamentos devido à CONTRATADA, no prazo e condições indicadas neste instrumento;

7.3. A CONTRATANTE deverá notificar a CONTRATADA, fixando-lhe prazo para proceder à correção dos serviços e/ou produtos que, dentro do prazo da garantia, apresentar defeitos e/ou irregularidades, devendo os mesmos ser refeitos e/ou corrigidos, com as mesmas características e qualificações exigidas no edital convocatório.

7.4. A CONTRATANTE deverá expedir, através da Secretaria Municipal de Administração e Planejamento, atestado de inspeção dos serviços e produtos quando de sua entrega, que servirá de instrumento de avaliação do cumprimento das obrigações contratuais.

7.5. Indicar formalmente o servidor responsável pela fiscalização dos serviços.

Cláusula 8ª - DAS PENALIDADES

8.1. O atraso injustificado na execução do objeto desta licitação, sem prejuízo do disposto no § 1º, do artigo 86, da Lei Federal Nº: 8666/93 e alterações sujeitará a CONTRATADA à multa de mora, calculada por dia de atraso da obrigação não cumprida na seguinte proporção:

8.1.1. Atraso de até 30 (trinta) dias, multa de 0,1% (um décimo por cento) ao dia sobre o valor global deste contrato;

8.1.2. Atraso superior a 30 (trinta) dias, multa de 0,2% (dois décimos por cento) ao dia sobre o valor global deste contrato.

8.2. Pela inexecução total ou parcial do objeto desta licitação, poderão ser aplicadas a CONTRATADA as seguintes penalidades:

8.2.1. Multa de 10% (dez por cento) sobre o valor total ou parcial da obrigação não cumprida;

8.2.2. Aplicação de suspensão temporária para licitar e/ou contratar com a municipalidade e/ou declaração de inidoneidade, conforme previsto no artigo 87 da Lei Federal Nº: 8666/93 e alterações.

8.3. A penalidade aqui prevista é autônoma e sua aplicação cumulativa é regida pelo artigo 87, §§ 2º e 3º, da Lei Federal Nº: 8.666/93 e alterações.

8.4. O valor das multas aplicadas será devidamente corrigido pelo IGPM/FGV/SP – Índice Geral de Preços de Mercado da Fundação Getúlio Vargas/SP, até a data de seu efetivo pagamento, e recolhido aos cofres da PREFEITURA, dentro de 03 (três) dias úteis da data de sua cominação, mediante guia de recolhimento oficial, ou outro índice que vier a substituí-lo, a critério da PREFEITURA.

Cláusula 9ª - DA RESCISÃO CONTRATUAL

9.1. Este contrato será rescindido total ou parcialmente pela PREFEITURA, de pleno direito, em qualquer tempo, isento de qualquer ônus ou responsabilidade, independentemente de ação, notificação ou interpelação judicial, sem que à CONTRATADA, assista o direito a qualquer indenização, se esta:

9.1.1. Falir, entrar em concordata, tiver a sua empresa dissolvida ou deixar de existir;

9.1.2. Transferir, no todo ou em parte, o presente contrato, sem prévia autorização da PREFEITURA;

9.1.3. Paralisar as entregas durante um período de 10 (dez) dias consecutivos;

9.1.4. Sem justa causa (a critério da PREFEITURA), suspender a entrega dos serviços;

9.1.5. Agir com dolo ou culpa ou mediante simulação ou fraude na execução do contrato.

9.2. A CONTRATADA reconhece os direitos da PREFEITURA, em caso de rescisão administrativa, de acordo com o disposto no artigo 80, da Lei Federal Nº: 8.666/93 e alterações.

Cláusula 10ª - DOS RECURSOS FINANCEIROS

10.1. As despesas decorrentes da execução deste contrato correrão por conta das seguintes dotações orçamentárias:

10.1.1. Classificação:

10.1.1.1. 01.02. 08.243.0003. 2.502. (15) 33.90.39. – Outros Serviços de Terceiros – Pessoa Jurídica, com nota de reserva no valor de R\$ 3.251,85;

10.1.1.2. 01.03. 08.244.0004. 2.501. (20) 33.90.39. – Outros Serviços de Terceiros – Pessoa Jurídica, com nota de reserva no valor de R\$ 1.352,05;

10.1.1.3. 03.01. 04.122.0006. 2.504. (39) 33.90.39. – Outros Serviços de Terceiros – Pessoa Jurídica, com nota de reserva no valor de R\$ 73.259,10;

10.1.1.4. 04.01. 10.122.0007. 2.505. (52) 33.90.39. – Outros Serviços de Terceiros – Pessoa Jurídica, com nota de reserva no valor de R\$ 30.060,10;

10.1.1.5. 04.01. 10.301.0008. 2.510. (75) 33.90.39. – Outros Serviços de Terceiros – Pessoa Jurídica, com nota de reserva no valor de R\$ 6.264,35;

10.1.1.6. 04.01. 10.301.0012. 2.518. (107) 33.90.39. – Outros Serviços de Terceiros – Pessoa Jurídica, com nota de reserva no valor de R\$ 1.889,20;

10.1.1.7. 04.01. 10.302.0009. 2.507. (137) 33.90.39. – Outros Serviços de Terceiros – Pessoa Jurídica, com nota de reserva no valor de R\$ 2.099,65;

10.1.1.8. 04.01. 10.302.0009. 2.508. (152) 33.90.39. – Outros Serviços de Terceiros – Pessoa Jurídica, com nota de reserva no valor de R\$ 547,00;
10.1.1.9. 04.01. 10.302.0009. 2.509. (162) 33.90.39. – Outros Serviços de Terceiros – Pessoa Jurídica, com nota de reserva no valor de R\$ 1.078,70;
10.1.1.10. 04.01. 10.302.0010. 2.517. (176) 33.90.39. – Outros Serviços de Terceiros – Pessoa Jurídica, com nota de reserva no valor de R\$ 1.341,90;
10.1.1.11. 05.01. 12.365.0013. 2.520. (213) 33.90.39. – Outros Serviços de Terceiros – Pessoa Jurídica, com nota de reserva no valor de R\$ 5.393,10;

10.1.1.12. 05.01. 12.365.0013. 2.521. (225) 33.90.39. – Outros Serviços de Terceiros – Pessoa Jurídica, com nota de reserva no valor de R\$ 7.857,85;
10.1.1.13. 05.02. 12.361.0014. 2.522. (241) 33.90.39. – Outros Serviços de Terceiros – Pessoa Jurídica, com nota de reserva no valor de R\$ 22.178,10;
10.1.1.14. 06.01. 15.452.0020. 2.536. (326) 33.90.39. – Outros Serviços de Terceiros – Pessoa Jurídica, com nota de reserva no valor de R\$ 6.353,20;
10.1.1.15. 08.01. 27.812.0023. 2.558. (349) 33.90.39. – Outros Serviços de Terceiros – Pessoa Jurídica, com nota de reserva no valor de R\$ 2.082,85;
10.1.1.16. 09.01. 08.244.0021. 2.544. (368) 33.90.39. – Outros Serviços de Terceiros – Pessoa Jurídica, com nota de reserva no valor de R\$ 9.035,30;
10.1.1.17. 10.01. 06.181.0022. 2.554. (394) 33.90.39. – Outros Serviços de Terceiros – Pessoa Jurídica, com nota de reserva no valor de R\$ 3.043,10;
10.1.1.18. 10.01. 06.181.0022. 2.555. (398) 33.90.39. – Outros Serviços de Terceiros – Pessoa Jurídica, com nota de reserva no valor de R\$ 1.872,75;
10.1.1.19. 11.01. 13.392.0024. 2.560. (422) 33.90.39. – Outros Serviços de Terceiros – Pessoa Jurídica, com nota de reserva no valor de R\$ 8.195,05.;

10.2. As dotações acima elencadas são constantes do orçamento-programa para exercício econômico e financeiro de 2018 e as correspondentes para os exercícios seguintes, em caso de prorrogação contratual.

Cláusula 11ª - DOS REAJUSTES DE PREÇOS

11.1. Conforme dispõe a Lei Federal Nº: 8.880/94, os preços não sofrerão reajustes pelo prazo de 01 (um) ano, contado da data da celebração do contrato.

11.2. Na hipótese de prorrogação, e após o decurso do prazo contratado inicialmente, o preço será reajustado anualmente, a contar da data de assinatura do contrato, utilizando-se como parâmetro de reajuste os índices autorizados pela ANATEL.

11.3. Será mantido o equilíbrio econômico-financeiro original do contrato conforme prescreve a Lei Federal Nº: 8.666/93 e alterações, a ser recomposto no indicado pelos preços vigentes na data da apresentação da proposta, ou de formulação dos preços a que esta se referir, ou ainda da última revisão contratual caso esta tenha envolvido pactuação de novos preços.

Cláusula 12ª - DO SUPORTE LEGAL

12.1. Este contrato é regulamentado pelos seguintes dispositivos legais:

12.1.1. Constituição Federal;

12.1.2. Lei Orgânica Municipal;

12.1.3. Lei Federal Nº: 8.666/93;

12.1.4. Lei Federal Nº: 8.880/94;
12.1.5. Lei Federal Nº: 8.883/94;
12.1.6. Lei Federal Nº: 9.032/95;
12.1.7. Lei Federal Nº: 9.069/95;
12.1.8. Lei Federal Nº: 9.648/98;
12.1.9. Lei Federal Nº: 9.854/99;
12.1.10. Lei Complementar Nº: 123/2006;
12.1.11. Lei Federal Nº: 12.440/2011;
12.1.12. Lei Municipal Nº: 2.519/2014;
12.1.13. Lei Municipal Nº: 2.572/2015;
12.1.14. Lei Complementar Nº 147/2014;
12.1.15. Decreto nº 8.302, de 4 de setembro de 2014;
12.1.16. Portaria MF nº 358, de 5 de setembro de 2014;
12.1.17. Portaria Conjunta PGFN/RFB nº 1.751, de 2 de outubro de 2014;
12.1.18. Demais disposições legais passíveis de aplicação, inclusive, os princípios gerais de Direito.

Cláusula 13ª - DAS DISPOSIÇÕES GERAIS E FINAIS

13.1. Não será permitido o início dos serviços sem a emissão da respectiva Ordem de Serviço.

13.1.1. A CONTRATADA deverá designar, por escrito, no ato de recebimento da Ordem de Serviço, presposto que tenha poder para resolução de possíveis ocorrências durante a execução deste contrato, informando, pelo menos, o nome, telefone comercial e e-mail do mesmo.

13.2. Aplica-se, no que couber, o disposto no artigo 79, da Lei Federal Nº: 8.666/93, bem como outros dispositivos legais previstos na aludida Lei.

13.3. Para os casos omissos neste contrato prevalecerão as condições e exigências da respectiva licitação e demais disposições em vigor.

13.4. A CONTRATADA assume a exclusiva responsabilidade pelo pagamento de salários, encargos trabalhistas e previdenciários advindos da legislação vigente, sendo que o pessoal por ela designado para trabalhar na execução do objeto deste contrato, não terá vínculo empregatício algum com a PREFEITURA.

13.5. É VEDADA a subcontratação PARCIAL OU TOTAL.

13.6. A CONTRATADA assume total responsabilidade pela execução integral deste contrato, sem direito a qualquer ressarcimento por despesas decorrentes de custos não previstos em sua proposta quer decorrentes de erro ou omissão de sua parte.

13.7. A CONTRATADA é responsável pelos encargos fiscais e comerciais resultantes da execução deste contrato.

13.8. As dúvidas surgidas na aplicação deste contrato, bem como os casos omissos serão solucionados pela Secretaria de Administração e Planejamento, ouvidos os órgãos técnicos especializados, ou profissionais que se fizerem necessários.

13.9. Prevalecerá o presente contrato no caso de haver divergências entre ele e os documentos eventualmente anexados.

13.10. Fica eleito o Foro desta Comarca de Rio Claro/SP para solução em primeira instância, de quaisquer questões suscitadas na execução deste contrato não resolvidos administrativamente.

13.11. Lido e achado conforme assinam este instrumento, em 03 (três) vias de igual teor e forma, as partes e as testemunhas.

Rogério Pascon
Prefeito Municipal

Contratada

Testemunhas:

1. Danielle Zanardi Leão Silva;
2. Rafael Stabellini Colabone;

PREGÃO PRESENCIAL 19/2018

ANEXO VIII - TERMO DE CIÊNCIA E DE NOTIFICAÇÃO

CONTRATANTE: PREFEITURA DO MUNICÍPIO DE SANTA GERTRUDES

CONTRATADO: _____

CONTRATO Nº (DE ORIGEM): _____

OBJETO: prestação de serviços de telefonia, internet e segurança digital.

ADVOGADO (S)/ Nº OAB: (*) _____

Pelo presente TERMO, nós, abaixo identificados:

1. Estamos CIENTES de que:

- a) o ajuste acima referido estará sujeito a análise e julgamento pelo Tribunal de Contas do Estado de São Paulo, cujo trâmite processual ocorrerá pelo sistema eletrônico;
- b) poderemos ter acesso ao processo, tendo vista e extraindo cópias das manifestações de interesse, Despachos e Decisões, mediante regular cadastramento no Sistema de Processo Eletrônico, conforme dados abaixo indicados, em consonância com o estabelecido na Resolução nº 01/2011 do TCESP;
- c) além de disponíveis no processo eletrônico, todos os Despachos e Decisões que vierem a ser tomados, relativamente ao aludido processo, serão publicados no Diário Oficial do Estado, Caderno do Poder Legislativo, parte do Tribunal de Contas do Estado de São Paulo, em conformidade com o artigo 90 da Lei Complementar nº 709, de 14 de janeiro de 1993, iniciando-se, a partir de então, a contagem dos prazos processuais, conforme regras do Código de Processo Civil;
- d) Qualquer alteração de endereço – residencial ou eletrônico – ou telefones de contato deverá ser comunicada pelo interessado, peticionando no processo.

2. Damo-nos por NOTIFICADOS para:

- a) O acompanhamento dos atos do processo até seu julgamento final e consequente publicação;
- b) Se for o caso e de nosso interesse, nos prazos e nas formas legais e regimentais, exercer o direito de defesa, interpor recursos e o que mais couber.

LOCAL e DATA: _____

GESTOR DO ÓRGÃO/ENTIDADE:

Nome: _____

Cargo: _____

CPF: _____ RG: _____

Data de Nascimento: ____/____/____

Endereço residencial completo: _____

E-mail institucional: _____

E-mail pessoal: _____

Telefone(s): _____

Assinatura: _____

Responsáveis que assinaram o ajuste:

Pelo CONTRATANTE:

Nome: _____
Cargo: _____
CPF: _____ RG: _____
Data de Nascimento: ____/____/____
Endereço residencial completo: _____
E-mail institucional _____
E-mail pessoal: _____
Telefone(s): _____
Assinatura: _____

Pela CONTRATADA:

Nome: _____
Cargo: _____
CPF: _____ RG: _____
Data de Nascimento: ____/____/____
Endereço residencial completo: _____
E-mail institucional _____
E-mail pessoal: _____
Telefone(s): _____
Assinatura: _____

Advogado:

(*) Facultativo. Indicar quando já constituído, informando, inclusive, o endereço eletrônico.