SERVIÇO AUTÔNOMO DE ÁGUA E ESGOTO DE SÃO CARLOS

EDITAL DE PREGÃO ELETRÔNICO Nº 054/2018

- *PARTICIPAÇÃO EXCLUSIVA PARA ME E EPP* -

PROCESSO LICITATÓRIO Nº 2062/2018

TIPO: "MENOR PREÇO"

O **SERVIÇO AUTÔNOMO DE ÁGUA E ESGOTO DE SÃO CARLOS**, pessoa jurídica de direito público interno, com sede nesta cidade de São Carlos - SP, à Avenida Getúlio Vargas, nº 1.500, Jardim São Paulo, inscrita no CNPJ sob nº 45.359.973/0001-50, I.E. nº 637.271.909.116, torna público para conhecimento de todos os interessados que no dia e hora abaixo indicados, será realizada licitação na modalidade **PREGÃO ELETRÔNICO**, do tipo "**MENOR PREÇO**", que será regido pela Lei Federal nº 10.520/2002, pelo Decreto Municipal nº 151/2004, com aplicação subsidiária da Lei Federal nº 8.666/93 e suas alterações posteriores, Lei Complementar n° 123/06, e suas alterações posteriores, e, no que couber, pelo Decreto nº 5450/2005 e pelo Decreto Federal nº 8538/2015, além das demais disposições legais aplicáveis, e condições estabelecidas no presente Edital e seus Anexos.

O Pregão Eletrônico será realizado em sessão pública, por meio de sistema eletrônico de comunicação pela INTERNET. O sistema referido utiliza recursos de criptografia e de autenticação que asseguram condições adequadas de segurança em toda etapa do certame.

A informação dos dados para acesso deve ser feita na página inicial no site do Banco do Brasil S/A. www.bb.com.br, opção Licitações, ou diretamente e www.licitacoes-e.com.br.

O edital estará disponível gratuitamente nos sítios: www.saaesaocarlos.com.br e www.licitacoes-e.com.br.

ABERTURA DAS PROPOSTAS: às 09:00 horas do dia 23/08/2018.

INÍCIO DA SESSÃO DE DISPUTA DE PREÇOS: às 10:00 horas do dia 23/08/2018.

TEMPO DE DISPUTA NORMAL: 05 minutos, a etapa de lances da sessão pública será encerrada por decisão do Pregoeiro. Após o fechamento, transcorrerá período de tempo de 01 (um) segundo até 30 (trinta) minutos, aleatoriamente determinado pelo sistema eletrônico, findo o qual será automaticamente encerrada a recepção de lances.

FORMALIZAÇÃO DE CONSULTAS: Observando o prazo legal, o concorrente poderá formular pedidos de esclarecimento por mensagem eletrônica (e-mail), informando o número da licitação, até 03 (três) dias úteis anteriores à data fixada para abertura da sessão pública, através endereço eletrônico: pregoeiro@saaesaocarlos.com.br.

As consultas serão respondidas por e-mail, ou diretamente no site www.licitacoes-e.com.br, no campo "mensagens" no link correspondente a este pregão.
No campo "mensagens" serão disponibilizadas, além das respostas, outras informações que o Pregoeiro julgar importantes, razão pela qual os interessados no certame devem consultar o sítio com frequência.

REFERÊNCIA DE TEMPO: para todas as referências de tempo será considerado o horário de Brasília - DF.

Integram o presente Edital, os seguintes anexos:

ANEXO I – DO OBJETO E DO ORÇAMENTO ESTIMADO;

ANEXO II – MODELO DE PROPOSTA DE PREÇOS;

ANEXO III – DECLARAÇÃO DE ADEQUAÇÃO AO ARTIGO 7º – INCISO XXXIII DA CONSTITUIÇÃO FEDERAL;

ANEXO IV – DECLARAÇÃO DE INEXISTÊNCIA DE FATO IMPEDITIVO;

ANEXO V – DECLARAÇÃO DE MICROEMPRESA OU EMPRESA DE PEQUENO PORTE;

ANEXO VI – TERMO DE CIÊNCIA E NOTIFICAÇÃO;

ANEXO VII – TERMO DE REFERÊNCIA;

ANEXO VIII – MODELO DE ATESTADO DE VISITA TÉCNICA.

1. DO OBJETO:

1.1. A presente licitação tem por objeto a contratação de Serviço Especializado e aquisição de Appliance de Segurança de Rede, para atender as necessidades com a proteção dos equipamentos e das informações da Autarquia, conforme especificações e quantidades estabelecidas no **Anexo I e VII** do presente edital.

2. DO PROCEDIMENTO:

2.1. O Pregão Eletrônico será realizado em sessão pública, por meio da *INTERNET*, mediante condições de segurança - criptografia e autenticação - em todas as suas fases, com apoio técnico e operacional do Setor de Manutenção e Suporte Tecnológico do SAAE.

2.2. O certame será realizado através da utilização da opção "Licitações", do Portal Eletrônico do Banco do Brasil S/A, conforme acordo de cooperação técnica celebrado entre o BANCO DO BRASIL S/A e o SERVIÇO AUTÔNOMO DE ÁGUA E ESGOTO DE SÃO CARLOS.

2.3. Os trabalhos serão conduzidos pelo "Pregoeiro", com o suporte de sua equipe de apoio, os quais, juntamente com a autoridade competente do órgão promotor da licitação, formam o conjunto de operadores do sistema do Pregão Eletrônico.

3. CONDIÇÕES DE PARTICIPAÇÃO:

- EXCLUSIVO PARA MICROEMPRESAS E EMPRESAS DE PEQUENO PORTE -

3.1. Poderão participar desta licitação os interessados que atendam a todas as exigências constantes neste Edital e seus anexos, inclusive, quanto à documentação - sendo vedada a participação sob a forma de consórcio - e satisfaçam as disposições contidas nos incisos I e II do art. 3º da Lei Complementar nº 123/2006 – EXCLUSIVO PARA ME/EPP.

3.1.1. A participação nessas condições implica no reconhecimento de não se encontrar em nenhuma das situações previstas no parágrafo 4º do Artigo 3º, da Lei complementar 123/2006.

3.2. Estarão impedidos de participar da presente licitação:

3.2.1. Os interessados suspensos do direito de licitar com a Administração Municipal de São Carlos, no prazo e nas condições do impedimento;

3.2.2. Os interessados que tenham sido declarados inidôneos pela Administração Municipal, Estadual ou Federal, o que abrange a administração direta e indireta, as entidades com personalidade jurídica de direito privado sob o seu controle e as fundações por ela instituída e mantida, enquanto perdurarem os motivos determinantes da punição ou até que seja reabilitado perante a autoridade que aplicou a penalidade;

3.2.3. Os interessados que estão em regime de falência, dissolução, liquidação ou concurso de credores;

3.2.4. Empresas em forma de consórcios.

4. DO CREDENCIAMENTO NO SISTEMA E EFETIVA PARTICIPAÇÃO:

4.1. Para acesso ao sistema eletrônico, os interessados em participar do Pregão Eletrônico deverão dispor de chave de identificação e senha pessoal e intransferível, obtida junto às Agências do Banco do Brasil S/A sediadas no País.

4.2. O credenciamento do concorrente vencedor e de seu representante legal junto ao sistema eletrônico implica na responsabilidade legal pelos atos praticados e a capacidade técnica para realização das transações inerentes ao pregão eletrônico.

4.3. A chave de identificação e a senha terão validade de 01 (um) ano e poderão ser utilizadas em qualquer pregão eletrônico, salvo quando canceladas por solicitação do credenciado ou por iniciativa do Banco, devidamente justificado.

4.4. É de exclusiva responsabilidade do usuário o sigilo da senha, bem como seu uso em qualquer transação efetuada diretamente ou por seu representante, não cabendo ao Banco do Brasil S/A, ao provedor do sistema ou ao órgão promotor da licitação responsabilidade por eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros.

4.5. A participação no Pregão Eletrônico se dará por meio da digitação da senha pessoal e intransferível do representante credenciado e subsequente cadastramento da proposta de preços, exclusivamente por meio do sistema eletrônico, observados data e horário limite estabelecidos.

4.6. O encaminhamento de proposta pressupõe o pleno conhecimento e atendimento às exigências de habilitação previstas no Edital. O concorrente será responsável por todas as transações que forem efetuadas em seu nome no sistema eletrônico, assumindo como firmes e verdadeiras suas propostas e lances.

4.7. Caberá ao concorrente acompanhar as operações no sistema eletrônico durante a sessão pública do pregão, ficando responsável pelo ônus decorrente da perda de negócios diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão.

5. DO RECEBIMENTO E ABERTURA DAS PROPOSTAS E FORMULAÇÃO DOS LANCES:

5.1. As propostas serão recebidas (cadastradas) até o horário previsto, após o que terá início a sessão pública do pregão eletrônico, com a divulgação das propostas de preços recebidas, passando o Pregoeiro a avaliar sua aceitabilidade.

5.2. Aberta a etapa competitiva, os representantes dos concorrentes deverão estar conectados ao sistema para participar da sessão de lances. A cada lance ofertado o concorrente será imediatamente informado de seu recebimento e respectivo horário de registro e valor.

5.3. O concorrente somente poderá oferecer lance inferior ao último por ele ofertado e registrado pelo sistema.

5.4. Não serão aceitos dois ou mais lances de mesmo valor, prevalecendo o que for recebido e registrado em primeiro lugar.

5.5. Durante o transcurso da sessão pública, os concorrentes serão informados, em tempo real, do valor do menor lance registrado. O sistema não identificará o autor dos lances aos demais concorrentes, tampouco ao pregoeiro.

5.6. No caso de desconexão com o Pregoeiro no decorrer da etapa competitiva do Pregão, o sistema eletrônico poderá permanecer acessível aos concorrentes para a recepção dos lances, retomando o Pregoeiro, quando possível, sua atuação no certame, sem prejuízos dos atos realizados.

5.6.1. Quando a desconexão persistir por tempo superior a 10 (dez) minutos, a sessão do Pregão Eletrônico será suspensa e terá reinício somente após comunicação expressa aos concorrentes, através de mensagem eletrônica, via sistema, divulgando data e hora da reabertura da sessão.

5.7. Na disputa normal, a etapa de lances da sessão pública será encerrada por decisão do pregoeiro mediante aviso de fechamento iminente da fase inicial de lances, emitido pelo sistema eletrônico, após transcorrer o período de tempo extra de 01 (um) segundo até 30 (trinta) minutos, aleatoriamente determinado pelo sistema eletrônico, findo o qual será automaticamente encerrada a recepção de lances.

5.8. Após o encerramento da etapa de lances da sessão pública, o Pregoeiro poderá encaminhar pelo sistema eletrônico contraproposta ao concorrente que tenha apresentado lance mais vantajoso, para que seja obtida a melhor proposta, observado o critério de julgamento, não se admitindo negociar condições diferentes daquelas previstas no Edital. A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais concorrentes.

5.9. O sistema informará a proposta de menor preço imediatamente após o encerramento da etapa de lances, e será aberta automaticamente fase para considerações finais pelo pregoeiro, após a qual este encerrará o lote.

5.10. O sistema informará a proposta de menor preço imediatamente após o encerramento da etapa de lances, e será aberta automaticamente fase para considerações finais pelo pregoeiro, após a qual este encerrará o lote.

5.10.1. As etapas seguintes serão realizadas fora da sala de disputa, através de acesso identificado.

5.11. Caso não sejam apresentados lances, será verificada a conformidade entre a proposta de menor preço e valor estimado para a contratação.

5.11.1. Se houver duas ou mais propostas iniciais de mesmo valor, o sistema classificará como arrematante o concorrente que inseriu a proposta primeiro.

6. DA PROPOSTA:

6.1. A proposta deverá obedecer aos seguintes critérios:

6.1.1. Os preços deverão ser cotados em moeda corrente nacional, devendo o valor unitário

proposto corresponder à unidade solicitada (Unidade de Medida constante no Anexo I);

6.1.2. Excepcionalmente nos casos em que o valor unitário for inferior a um real, poderão ser aceitas propostas com 4 (quatro) casas decimais;

6.1.3. A proposta de preço contemplando o "valor global do lote" deverá ser cadastrada no sistema eletrônico até a data e hora marcada para abertura das propostas. Para participar do lote, o fornecedor deverá ofertar o valor correspondente à quantidade total de todos os itens inclusos no lote, conforme o Anexo I deste edital.

6.1.4. Após a sessão de disputa, deverá ser apresentada, pelo licitante classificado em primeiro lugar (arrematante do lote), **proposta escrita atualizada**, nos moldes estabelecidos no Anexo II, juntamente com a documentação de habilitação, conforme item 10 deste edital.

6.1.5. A marca/procedência dos equipamentos objeto do certame poderá ser especificada no envio da proposta junto ao site, em campo específico do site Licitações-e "Informações adicionais".

6.1.6. A marca/procedência dos equipamentos deverá ser obrigatoriamente especificada na proposta escrita.

6.1.7. O licitante arrematante deverá apresentar, **juntamente com a proposta escrita**, certificados, prospectos ou catálogos com referências técnicas, sendo que, pelos quais, seja possível comprovar a conformidade do Projeto e Serviços ofertados com o especificado no edital e seus anexos (especificamente, conforme a planilha do Anexo II e as especificações do Anexo VII).

6.1.8. Se o arrematante for o fabricante do(s) equipamento(s), deverá permitir visita de representante da Autarquia às instalações, caso esta ache necessário.

6.1.9. Condições de pagamento, conforme item 13 deste edital e seus subitens.

6.2. O prazo de validade da proposta é de, no mínimo, 60 (sessenta) dias a contar da data de sua apresentação.

6.3. Prazo e condições de entrega: Os equipamentos deverão ser entregues no máximo 30 (trinta) dias corridos após a assinatura do contrato ou recebimento de termo análogo, bem como os serviços deverão iniciar em até 15 (quinze) dias corridos após a entrega dos equipamentos, conforme o item 18 do **Anexo VII**, efetivando-se no Setor de Almoxarifado, à Rua José Casale, 400, Jardim São Paulo - São Carlos - SP, CEP 13570-450, horário das 8h às 11h e das 13h às 16h, de segunda-feira a sexta-feira, exceto feriados e pontos facultativos, por conta, risco e custo do Contratado, incluído todos os custos e despesas, tais como, e sem se limitar a: custos diretos e indiretos, tributos incidentes, despesas administrativas, materiais, serviços, encargos sociais, trabalhistas, seguros, frete, embalagens, carga/descarga, lucro, despesas, acessórios e encargos, inclusive tributários, incidente sobre a proposta, quando não incorporados ao preço oferecido e outros necessários ao cumprimento integral do objeto deste edital e seus anexos.

6.3.1. O licitante contratado ficará obrigado a trocar, às suas expensas, os equipamentos do objeto do certame, que estiverem em desacordo com as exigências do edital e/ou apresentar irregularidades, no prazo máximo de 10 (dez) dias úteis, após comunicação do SAAE feita via ofício, fac-símile ou e-mail.

6.3.2. O licitante contratado, de acordo com a cláusula 2ª, inciso I, do protocolo ICMS 42, estará obrigado a emitir Nota Fiscal Eletrônica - NF-E, modelo 55, portanto, além da via

original que acompanha a mercadoria, encaminhar também por meio eletrônico para o seguinte endereço de e-mail: almoxarifado@saaesaocarlos.com.br.

6.4. Garantia: A CONTRATADA deverá atender a toda solicitação da CONTRATANTE, quando está necessitar de suporte técnico, bem como a troca de algum equipamento, conforme os itens 16, 17 e 20 do Anexo VII; por um período de 12 (doze) meses, após o Sistema entrar em funcionamento.

6.5. É de inteira responsabilidade do concorrente o preço e demais condições apresentadas, salvo se no momento da abertura da proposta for alegado erro, e aceito pelo Pregoeiro, será registrado em ata, devendo o lote ser desconsiderado da proposta.

6.6. No caso de discordância entre os preços unitários e totais, prevalecerá a soma dos unitários.

6.7. Serão desclassificadas as propostas que conflitem com as normas deste edital ou da legislação em vigor.

6.8. Igualmente serão desclassificadas as propostas que:

6.8.1. Sejam incompletas, isto é, não contenham informação(ões) suficiente(s) que permita(m) a perfeita especificação do equipamento licitado;

6.8.2. Contenham qualquer limitação ou condição substancialmente contrastante com o presente Edital, ou seja, manifestamente inexequíveis, por decisão do Pregoeiro.

6.8.3. Com garantia dos equipamentos inferiores à do fabricante.

6.9. O Município é considerado consumidor final, sendo que o licitante deverá obedecer ao fixado no art. 155, §2º, VII, b, da Constituição Federal de 1988.

7. DO VALOR ESTIMADO:

7.1. O valor estimado para a presente contratação é de **R$ 70.322,34 (setenta mil, trezentos e vinte e dois reais e trinta e quatro centavos).**

8. DOS CRITÉRIOS DE JULGAMENTO:

8.1. Para julgamento, será adotado o critério de "MENOR PREÇO TOTAL DO LOTE", observados os prazos para fornecimento, as especificações técnicas, parâmetros mínimos de desempenho, qualidade e demais condições definidas neste Edital e seus Anexos I e VII.

8.2. O Pregoeiro anunciará o concorrente detentor da proposta ou lance de menor valor após o encerramento da etapa de lances da sessão pública ou, quando for o caso, após negociação e decisão pelo Pregoeiro acerca da aceitação do lance de menor valor.

8.3. Se a proposta ou o lance de menor valor não for aceitável, o Pregoeiro examinará a proposta ou o lance subsequente, na ordem de classificação, verificando a sua aceitabilidade e procedendo a sua habilitação. Se for necessário, repetirá esse procedimento, sucessivamente, até a apuração de uma proposta ou lance que atenda ao edital.

8.4. Ocorrendo a situação a que se referem os itens 8.2 e 8.3 deste Edital, o Pregoeiro poderá negociar com o concorrente para que seja obtido melhor preço.

8.5. Os concorrentes, ainda que não classificados em primeiro lugar, deverão consultar o sistema regularmente para verificar se passaram à condição de arrematante do lote, em

função de desclassificação ou inabilitação do arrematante anterior, podendo o pregoeiro retomar a negociação pelo sistema, e convocá-los a apresentar os documentos de habilitação.

8.6. Da sessão, o sistema gerará ata circunstanciada, na qual estarão registrados todos os atos do procedimento e as ocorrências relevantes.

8.6.1. Quando necessário o Pregoeiro e a equipe de apoio poderão complementar as informações da ata gerada pelo sistema do Banco do Brasil, por meio de ata interna que será juntada aos autos referente ao certame.

9. DO JULGAMENTO FINAL:

9.1. O(s) licitante(s) que apresentar(em) menor preço, objeto do presente certame, bem como a documentação exigida em ordem, será(ão) considerado(s) vencedor(es).

10. DA HABILITAÇÃO:

10.1. O(s) licitante(s) arrematante(es) deverá(ão) apresentar a documentação abaixo relacionada da seguinte maneira: **digitalizada**, no prazo de até 04 (quatro) horas da confirmação de arrematação, via correio eletrônico para pregoeiro@saaesaocarlos.com.br; **e também os originais ou fotocópias autenticadas**, no prazo máximo de 02 (dois) dias úteis, no Setor de Contratos e Licitações do SAAE, localizado à Avenida Getúlio Vargas, 1500 - Jardim São Paulo - CEP: 13570-390 - São Carlos - SP, aos cuidados do pregoeiro.

10.1.1. Juntamente com os documentos de habilitação deverá ser apresentada a proposta escrita com o valor atualizado (valor arrematado/ negociado), bem apresentar todos os catálogos impressos, em português ou em inglês, da solução apresentada.

10.1.2. Os documentos relativos à habilitação deverão ser entregues em envelope fechado e poderão ser apresentados em original, por qualquer processo de cópia autenticada por cartório competente ou publicação em órgão da Imprensa Oficial. **No(s) envelope(s) deverá haver a identificação do número do pregão eletrônico, o nome do pregoeiro responsável, bem como os dados da empresa.**

10.2. A participação no presente certame implica no reconhecimento da inexistência de fato impeditivo posterior ou anterior, à expedição dos documentos apresentados para habilitação, observado o disposto no Artigo 43, parágrafo 1º da Lei complementar 123/06.

10.2.1. A comprovação de regularidade fiscal e trabalhista das microempresas e empresas de pequeno porte somente será exigida para efeito de contratação e não como condição para participação no certame. No entanto, deverão elas apresentar os documentos referentes à regularidade fiscal e trabalhista, mesmo que este apresente alguma restrição.

10.2.2. Havendo alguma restrição na comprovação da regularidade fiscal e trabalhista de microempresas e empresas de pequeno porte, será assegurado o prazo de 05 (cinco) dias úteis, a contar da data da divulgação do resultado da habilitação, via chat, na página do pregão, para a regularização da documentação, pagamento ou parcelamento do débito e apresentação de eventuais certidões negativas ou positivas com efeito de negativa, após o que, a licitante será declarada vencedora, e dar-se-á início à fase recursal.

10.2.3. A não regularização da documentação, no prazo previsto acima, implicará na decadência do direito à contratação, sem prejuízo das sanções legais, procedendo-se a convocação dos demais licitantes para retomar os atos referentes ao procedimento licitatório.

10.3. Se o licitante desatender as exigências habilitatórias, o pregoeiro examinará a proposta subsequente, verificando a sua aceitabilidade e procederá conforme a ordem de classificação, e assim sucessivamente, até a apuração de uma proposta que atenda ao edital.

10.4. OS DOCUMENTOS DE HABILITAÇÃO SÃO OS SEGUINTES:

10.4.1 – Habilitação Jurídica:

a) Registro comercial, no caso de empresa individual;

b) Ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado na Junta Comercial, em se tratando de sociedades comerciais;

c) Documentos de eleição dos atuais administradores, tratando-se de sociedades por ações, acompanhados da documentação mencionada na alínea "b", deste subitem;

d) Inscrição do ato constitutivo, no caso de sociedades civis, acompanhada de prova de diretoria em exercício;

e) Decreto de autorização e ato de registro ou autorização para funcionamento expedido pelo órgão competente, tratando-se de empresa ou sociedade estrangeira em funcionamento no país, quando a atividade assim o exigir.

10.4.2 – Regularidade Fiscal e Trabalhista:

a) Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas (CNPJ);

b) Prova de inscrição no cadastro de contribuintes estadual ou municipal, relativo ao domicílio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

c) Prova de Regularidade para com a Fazenda Federal e Prova de Regularidade Relativa à Seguridade Social mediante apresentação de: Certidão Negativa de Débitos Relativos a Tributos Federais e à Dívida Ativa da União, ou Certidão Positiva com Efeitos de Negativa, expedida pela Secretaria da Receita Federal e Procuradoria-Geral da Fazenda Nacional, com validade na data da apresentação, referente a tributos mobiliários, na forma da Lei.

d) Prova de Regularidade para com a Fazenda Estadual: Certidão Negativa de Débitos, ou Certidão Positiva com efeitos de Negativa, com validade na data da apresentação, referente a tributos mobiliários, na forma da Lei.

e) Prova de Regularidade para com a Fazenda Municipal: Certidão Negativa de Débitos, ou Certidão Positiva com efeitos de Negativa, do domicílio ou sede do concorrente, ou outra equivalente na forma da Lei, com validade na data da apresentação, referente a tributos mobiliários, na forma da Lei.

f) Prova de regularidade relativa ao FGTS - (CRF) - Fundo de Garantia por Tempo de Serviço, com validade na data da apresentação.

g) Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante apresentação de Certidão Negativa ou Positiva com efeitos de Negativa de Débitos Trabalhistas, em nome do licitante, com validade na data de apresentação, na forma da Lei.

10.4.3 – Capacidade Técnica:

a) Atestado(s) fornecido(s) por pessoa jurídica de direito público ou privado de desempenho

anterior que comprove a capacidade para execução do objeto desta licitação, podendo tal comprovação ser efetuada por 01 (um) ou mais atestados, admitindo-se prova de execução similares em quantidades razoáveis, assim, consideradas 50% a 60% do fornecimento pretendido.

10.4.4 – Qualificação Econômica Financeira:

a) Certidão Negativa de Falência, expedida pelo distribuidor da sede da pessoa jurídica com data de expedição não superior a 90 (noventa) dias da data da abertura da licitação. Caso conste no documento a data de validade, esta prevalecerá.

b) Em caso de Recuperação Judicial, deverá ser apresentado o Plano de Recuperação já homologado pelo Juízo competente e em pleno vigor.

10.4.5 – Outras Comprovações:

a) Declaração que de acordo com o Art. 7º inciso XXXIII da Constituição Federal/1988, não emprega menores de 16 anos, salvo na condição de aprendiz, ou menores de 18 anos em trabalho noturno, perigoso ou insalubre, conforme o constante do Anexo III.

b) Declaração de pleno atendimento aos requisitos de habilitação e inexistência de qualquer fato impeditivo à participação, conforme o constante do Anexo IV.

c*) No caso de Microempresa ou Empresa de Pequeno Porte que optar pelos benefícios da Lei Complementar nº 123/06, apresentar declaração de enquadramento nessas situações conforme o constante do Anexo V, e deverá também ser apresentada uma das seguintes comprovações**:**

1) Quando optante pelo Simples Nacional: comprovante da opção pelo simples obtido no sítio da Secretaria da Receita Federal;

2) Quando não optante pelo Simples Nacional: prova através de documento expedido através da junta comercial ou balanço patrimonial e Demonstração do Resultado do Exercício – DRE, comprovando ter receita bruta dentro dos limites estabelecidos nos incisos I e II, do Artigo 3º, da Lei complementar 123/06;

***A** participação nas condições previstas nesta alínea, implica no reconhecimento de não se encontrar em nenhuma das situações previstas no parágrafo 4º do Artigo 3º, da Lei complementar 123/06.

10.5. Os licitantes cadastrados no SAAE poderão deixar de apresentar os documentos **originais** que já constem do respectivo cadastro (os que ainda estiverem dentro do prazo de validade), devendo os demais ser encaminhados observados os prazos e condições estabelecidos neste edital.

10.6. Os documentos apresentados deverão ser, obrigatoriamente, da mesma sede, ou seja, se da matriz, todos da matriz, se de alguma filial, todos da mesma filial, com exceção dos documentos que são válidos para matriz e todas as filiais.

10.6.1. Caso a licitante pretenda que um de seus estabelecimentos (filiais), que não o participante da licitação, execute o futuro contrato, deverá apresentar toda a documentação de ambos os estabelecimentos na forma e condições previstas neste edital.

10.7. Havendo recurso, o pregoeiro apreciará os mesmos e, caso não reconsidere sua posição, caberá à autoridade máxima competente a decisão em grau final.

10.8. Após a habilitação, poderá a concorrente ser desclassificada por motivo relacionado com a capacidade jurídica, regularidade fiscal, qualificação econômico-financeira, qualificação técnica e/ou inidoneidade, em razão de fatos supervenientes ou somente conhecidos após o julgamento.

10.9. Todos os documentos e certidões deverão ser apresentados dentro do respectivo prazo de validade.

11. DA IMPUGNAÇÃO AO EDITAL E RECURSOS:

11.1. Decairá do direito de impugnação dos termos do Edital de Pregão, perante o SAAE, aquele que não se manifestar até 02 (dois) dias úteis antes da data de abertura da sessão do pregão, apontando as falhas e irregularidade que o viciariam.

11.1.1. A impugnação poderá ser feita através do e-mail: pregoeiro@saaesaocarlos.com.br, devendo conter todos os dados da impugnante (nome, CNPJ, endereço e e-mail) para competente resposta.

11.1.2. A apresentação de impugnação, após o prazo estipulado no subitem anterior, não a caracterizará como recurso, recebendo tratamento como mera informação.

11.2. A sessão pública compreende, sucessivamente, a abertura das propostas, a etapa de lances e a declaração do vencedor.

11.2.1. A declaração do vencedor compreende a análise da proposta e o julgamento de habilitação, de acordo com as exigências previstas neste Edital.

11.3. De todos os atos e decisões do Pregoeiro, relacionados ao pregão, cabe recurso;

11.3.1. Depois de declarado o vencedor, no sistema, qualquer concorrente poderá, durante a sessão pública, de forma imediata e motivada, em campo próprio do sistema, manifestar sua intenção de recorrer, com o registro da síntese de suas razões, sendo-lhes facultado apresentar as razões de recurso, no prazo de 03 (três) dias úteis, ficando os demais, desde logo, intimados para, querendo, apresentarem contrarrazões em igual prazo, que começará a contar do término do prazo do recorrente, sendo-lhes assegurada vista dos elementos indispensáveis à defesa dos seus interesses.

11.3.1.1. Encerrada a etapa de lances, os concorrentes deverão consultar regularmente o sistema para verificar se foi declarado o vencedor e se está aberta a opção para interposição de recurso. A partir da liberação, os licitantes terão 24 (vinte e quatro) horas para manifestarem sua intenção de recorrer, com o registro da síntese de suas razões, em campo próprio do sistema.

11.3.1.2. O recurso contra atos e decisões do pregoeiro terá efeito suspensivo e o seu acolhimento importará a invalidação apenas dos atos insuscetíveis de aproveitamento.

11.4. A falta de manifestação imediata e motivada do concorrente quanto à intenção de recorrer, importará na decadência desse direito, ficando o pregoeiro autorizado a adjudicar o objeto ao concorrente declarado vencedor.

11.4.1. Caso a adjudicação ao concorrente vencedor não seja proferida na própria sessão, o prazo de recurso passará a contar a partir da publicação do resultado do certame no Diário Oficial do Município (www.saocarlos.sp.gov.br).

11.5. Os recursos deverão ser endereçados ao SAAE e seu encaminhamento se dará por intermédio do pregoeiro.

11.6. Não serão conhecidos as impugnações e os recursos apresentados fora do prazo legal e/ou subscritos por representante não habilitado ou não identificado no processo para responder pelo concorrente.

11.7. No julgamento da habilitação e das propostas, o pregoeiro poderá sanar erros ou falhas que não alterem a substância das propostas, dos documentos e sua validade jurídica, mediante despacho fundamentado, registrado em ata e acessível a todos, atribuindo-lhes validade e eficácia para fins de habilitação e classificação, inclusive através de verificação junto aos sítios oficiais e certificados.

11.8. Cabe, ainda, recurso contra a decisão que:

a) Anular ou revogar o pregão;
b) Determinar a aplicação das penalidades de advertência, multa, suspensão temporária do direito de licitar e contratar com o SAAE.

11.8.1. Os recursos de que tratam as letras "a" e "b" do item 11.8 deverão ser interpostos no prazo de 05 (cinco) dias úteis a contar da intimação do ato, e terão efeito suspensivo;

11.8.1.1. A intimação dos atos referidos no item 15 será feita mediante publicação na imprensa oficial e terá efeito suspensivo.

11.8.1.2. Interposto o recurso de que tratam as letras "a" e "b" do item 11.8, será comunicado aos demais concorrentes, que poderão impugná-lo no prazo de 05 (cinco) dias úteis.

11.8.2. Os recursos interpostos fora do prazo não serão conhecidos.

11.8.3. O recurso será dirigido à autoridade superior, por intermédio da que praticou o ato recorrido, a qual poderá reconsiderar a sua decisão, no prazo de 05 (cinco) dias úteis, ou nesse mesmo prazo fazê-lo subir, devidamente informado, devendo, nesse caso, a decisão ser proferida no prazo de 05 (cinco) dias úteis, contado do recebimento do recurso.

12. DA HOMOLOGAÇÃO E CONTRATAÇÃO:

12.1. Decididos os recursos e constatada a regularidade dos atos procedimentais, a autoridade competente homologará os procedimentos licitatórios e adjudicará o objeto ao vencedor.

12.2. Adjudicada a licitação pela autoridade competente, o adjudicatário será convocado para assinar o contrato ou retirar o instrumento equivalente no prazo de 05 (cinco) dias úteis. Caso nos documentos de habilitação não estejam contemplados todos os dados do representante legal que assinará o Contrato, deverá o licitante vencedor encaminhar as informações e comprovações no prazo para entrega dos documentos no original ou cópia autenticada, previsto no item 10.1.

12.3. Como condição para a sua contratação, o concorrente vencedor deverá manter as condições de habilitação, prestar as informações solicitadas pela contratante dentro dos prazos estipulados, bem como não transferir a outrem as obrigações decorrentes desse contrato/instrumento equivalente.

12.4. A obrigação decorrente do fornecimento de bens será firmada entre a Administração e o Fornecedor, por meio de contrato ou instrumento equivalente, observando as condições estabelecidas neste Edital, e na legislação vigente.

12.5. Quando o concorrente vencedor convocado dentro do prazo de validade da sua

proposta, não celebrar o contrato/instrumento equivalente ou não apresentar situação regular no ato da assinatura deste, sem motivo justo e aceito pelo Contratante, será facultada a convocação do outro concorrente, observada a ordem de classificação para celebrar o contrato/instrumento equivalente, e assim sucessivamente, sem prejuízo da aplicação das sanções cabíveis.

12.6. O objeto contratual poderá ser acrescido ou reduzido de acordo com o disposto no Art. 65, § 1º, da Lei nº 8.666/93 e alterações posteriores.

13. DO PAGAMENTO:

13.1. Liquidadas as despesas através do recebimento definitivo acompanhado dos documentos exigidos do Edital, será processado o respectivo pagamento.

13.2. Os pagamentos serão efetuados mediante crédito em conta corrente devendo o concorrente informar o número do banco, da agência e conta bancária, ou através de banco credenciado, a critério do SAAE.

13.3. O pagamento será efetuado 30 (trinta) dias corridos contados do recebimento do objeto licitado, acompanhado da Nota Fiscal Fatura, e apresentação dos comprovantes de regularidade perante o INSS e FGTS, desde que devidamente atestado pelo SAAE, através de Termo de Recebimento Provisório/Definitivo (Resolução SAAE 03/2016).

14. DO RECURSO ORÇAMENTÁRIO:

14.1. As despesas decorrentes com a presente aquisição correrão por conta de Dotação Orçamentária nº 060100.1751250012.503 – 44905200 e 33903900; fonte: Recursos Próprios da Administração Indireta.

15. DAS SANÇÕES ADMINISTRATIVAS:

15.1. O licitante que incorrer nas infrações previstas no Artigo 7º da Lei 10.520, de 17 de Julho de 2002, ficará sancionado nos termos abaixo dispostos:

a) Apresentar documento falso exigido para o certame: impedimento de contratar com a Administração Pública, por até 5 (cinco) anos;
b) Ensejar o retardamento da execução do certame, valendo-se de meios ilícitos: impedimento de contratar com o SAAE, por até 5 (cinco) anos;
c) Não manter a proposta ou não celebrar o contrato ou retirar o instrumento equivalente: impedimento de contratar, por até 2 (dois) anos, com o SAAE;
d) Falhar na execução do contrato: impedimento de contratar, por até 3 (três) anos, com o SAAE;
e) Fraudar na execução do objeto contratual: impedimento de contratar, por até 5 (cinco) anos, com a Administração Pública;
f) Comportar-se de modo inidôneo ou cometer fraude fiscal: impedimento de contratar, por até 5 (cinco) anos, com a Administração Pública.

Parágrafo Único: No processo administrativo serão garantidos ampla defesa e o contraditório.

15.2. O licitante sujeitar-se-á, ainda, as sanções de: advertência, multa, impedimento de contratar e declaração de inidoneidade, que poderão ser cumuladas com multa, sem prejuízo da rescisão contratual.

15.3. As multas poderão ser cumulativas, reiteradas e aplicadas em dobro, sempre que se repetir o motivo.

15.4. No descumprimento de quaisquer obrigações licitatórias/contratuais, bem como o descumprimento da regularização no exercício do direito previsto no subitem 10.2.2, poderá ser aplicada multa indenizatória de até 10% (dez por cento) do valor total do objeto licitado.

15.5. As multas serão, após regular processo administrativo, descontadas da(s) fatura(s), cobrada judicialmente ou extrajudicialmente, a critério do SAAE.

15.6. Da intenção de aplicação de quaisquer das penalidades previstas, será concedido prazo para defesa prévia de 05 (cinco) dias úteis a contar da notificação.

15.7. Da aplicação da sanção caberá recurso no prazo de 05 (cinco) dias úteis a contar da publicação no Diário Oficial do Município de São Carlos - SP.

15.8. As penalidades serão obrigatoriamente registradas no Cadastro de Fornecedores do SAAE. No caso de impedimento do direito de licitar e contratar ou declaração inidoneidade, o licitante terá seu cadastro cancelado por igual período.

15.9. A recusa do licitante vencedor em retirar e devolver devidamente assinado o contrato/instrumento equivalente no prazo estabelecido importará na decadência e aplicação de multa correspondente a 10% sobre o valor constante da proposta.

15.10. O Contrato ou documento equivalente poderá ser rescindido nas situações previstas nos artigos 77 e 78 da Lei nº 8.666/93 e alterações posteriores.

16. DAS DISPOSIÇÕES FINAIS:

16.1. A participação do presente certame implica no reconhecimento da inexistência de qualquer fator impeditivo à participação inclusive punição de impedimento ou inidoneidade para licitar e contratar com a Administração Pública.

16.2. As normas disciplinadoras deste Pregão serão sempre interpretadas em favor da ampliação da disputa entre os interessados, desde que não comprometam o interesse da Administração, a finalidade e a segurança da contratação.

16.3. É facultada ao Pregoeiro, ou à autoridade superior, em qualquer fase da licitação, a promoção de diligência destinada a esclarecer ou complementar a instrução do processo, vedada a inclusão posterior de documento ou informação que deveria constar no ato da sessão pública.

16.4. A autoridade competente para determinar a assinatura do Contrato e posteriores contratações, poderá revogar a licitação em face de razões de interesse público, derivadas de fato superveniente devidamente comprovado, pertinente e suficiente para justificar tal conduta, devendo anulá-la por ilegalidade, de ofício ou por provocação de qualquer pessoa, mediante ato escrito e fundamentado.

16.5. Os licitantes não terão direito à indenização em decorrência da anulação do procedimento licitatório.

16.6. A Administração reserva-se no direito de transferir o prazo para o recebimento e abertura das propostas, descabendo em tais casos, direito à indenização pelos licitantes.

16.7. A participação no presente certame implica em concordância tácita, por parte do

licitante, com todos os termos e condições deste Edital e seus Anexos.

16.8. Todos os atos que demandem publicidade em imprensa oficial serão publicados no Diário Oficial do Município de São Carlos, ressalvada a hipótese do art. 21, §4º, da Lei 8.666/93.

16.9. Fica eleito o Foro da Comarca de São Carlos - SP, para dirimir litígios resultantes deste Edital e seus Anexos.

São Carlos, 08 de agosto de 2018.

Marcel Rodrigo dos Santos
Pregoeiro
Portaria nº 059/2017

ANEXO I
DO OBJETO E DO ORÇAMENTO ESTIMADO

LOTE 01				
Item	**Descrição**	**Qt.**	**Un.**	**Valor Estimado Total do Item**
01	Appliance para Segurança de rede de dados - Next Generation Firewall UTM. **(Para elaboração do valor do Objeto, vide planilha do Anexo II.)**	01	PÇ	R$ 70.322,34
VALOR ESTIMADO TOTAL DO LOTE 01				**R$ 70.322,34**

***** PÇ = peça(s);

ANEXO II
MODELO DE PROPOSTA DE PREÇOS

Pregão Eletrônico nº _____/2018

Ao SAAE - SERVIÇO AUTÔNOMO DE ÁGUA E ESGOTO DE SÃO CARLOS - SP.

Prezados Senhores:

A EMPRESA_____, com endereço na Rua _____, nº _____, na cidade de _____, (UF), telefone para contato (DDD) _____, e-mail: _____, neste ato representada pelo seu (sócio/diretor/proprietário), _____, portador do RG nº _____ e CPF nº _____, inscrita no CNPJ/MF nº _____, Inscrição Estadual nº _____ e Inscrição Municipal nº _____, tendo examinado minuciosamente o Edital em epígrafe e seus Anexos (especificamente o **Anexo VII**) e, com o conhecimento das condições estabelecidas, reconhecendo a inexistência de fato impeditivo, formula a seguinte PROPOSTA:

LOTE 01					
(PROJETO BÁSICO)					
ITEM	DESCRIÇÃO	MARCA/ FABRICATE	QUANTIDADE ANUAL	PREÇO UNITÁRIO (R$)	PREÇO TOTAL (R$)
01	Appliance UTM atualização, conforme especificações no Anexo VII.		01		
02	Servidor físico para registro e armazenamento de LOG´s de usuários, conforme especificações no Anexo VII.		01		
03	Ponto de acesso sem fio (AP WiFi), conforme especificações no Anexo VII.		01		
(SERVIÇOS)					
04	Licenças Appliance UTM atualização e garantia por 12 meses ou mais.	Serviços	01		
05	Suporte dos UTM On Site e remoto (8x5) por 12 meses ou mais.	Serviços	01		
06	Suporte dos UTM On Site e remoto (8x5) por 12 meses ou	Serviços	01		

	mais.				
07	Treinamento do UTM (02 técnicos no mínimo).	Serviços	01		
				VALOR TOTAL DO LOTE 01	
VALOR TOTAL DA PROPOSTA: R$					

Preço total por extenso:
Prazo de entrega e início dos serviços:
Garantias:
Validade da Proposta:
Condições de Pagamento:
Nome do Banco, Ag. e nº C/Corrente:

Obs.: Nos preços estão inclusos quaisquer ônus tais como, tributos, taxas administrativas, impostos, fretes, seguros e demais encargos, despesas com entrega dos valores dos materiais, da mão de obra utilizada, dos veículos, equipamentos, dos encargos sociais e fiscais, das ferramentas, aparelhos, instrumentos, da água e energia elétrica, da segurança e vigilância, dos ônus diretos e indiretos, da administração, do lucro e de quaisquer outras despesas incidentes sobre os serviços, e outras necessárias à perfeita execução do projeto.

Declaramos que, esse fornecimento será efetuado em conformidade com as condições constantes do Edital de Pregão na forma Eletrônica nº _____/2018 e seus anexos, o qual conhecemos e aceitamos em todos os seus termos.

Declaramos ainda que o representante legal de nossa empresa que assinará o Contrato ou instrumento equivalente é o Sr. (a)_____ portador(a) do RG nº_____ e do CPF nº_____.

Local,_____de_____de 2018

_____
Assinatura/Nome/Cargo

ANEXO III

DECLARAÇÃO DE ADEQUAÇÃO AO ARTIGO 7º INCISO XXXIII DA CONSTITUIÇÃO FEDERAL

(Nome da empresa), CNPJ nº_____, sediada (endereço completo), por seu representante legal, abaixo subscrito, DECLARA EXPRESSAMENTE que não emprega menor de dezoito anos em trabalho noturno, perigoso ou insalubre; bem como não emprega menor de dezesseis anos ou o emprega na condição de aprendiz e, ainda não emprega, em hipótese alguma, menor de quatorze anos.

Local e data

Nome do representante legal
RG nº.....

ANEXO IV

DECLARAÇÃO DE INEXISTÊNCIA DE FATO IMPEDITIVO

Eu_____(nome completo), RG nº _____, representante legal da_____(denominação da empresa jurídica), CNPJ nº_____ DECLARO, sob as penas da lei, que a empresa cumpre plenamente as exigências e os requisitos de habilitação previstos no instrumento convocatório do Pregão nº_____/2018, realizado pelo Serviço Autônomo de Água e Esgoto de São Carlos, inexistindo qualquer fato impeditivo de sua participação neste certame, estando ciente da obrigatoriedade de declarar ocorrências posteriores.

Local e data

Nome do representante legal
RG nº.....

ANEXO V

DECLARAÇÃO DE MICROEMPRESA OU EMPRESA DE PEQUENO PORTE

Para fins de participação na licitação (indicar o nº do Edital), a(o) (nome completo do proponente)....., CNPJ, sediada (o).....(endereço completo), DECLARA, sob as penas da lei, que cumpre os requisitos legais para a qualificação como (Microempresa ou Empresa de Pequeno Porte, conforme o caso), na forma da Lei Complementar nº 123, de 14.12.2006, estando apta a usufruir do tratamento favorecido estabelecido nos arts. 42 a 49 daquela Lei Complementar.

DECLARA, ainda, que não existe qualquer impedimento entre os previstos nos incisos do § 4º do artigo 3º da Lei Complementar nº 123/2016.

Local e data

Nome do representante legal
RG nº.....

ANEXO VI

TERMO DE CIÊNCIA E NOTIFICAÇÃO

CONTRATANTE: SERVIÇO AUTÔNOMO DE ÁGUA E ESGOTO DE SÃO CARLOS - SAAE
CONTRATADA: _____
CONTRATO Nº: _____/2018
OBJETO: Aquisição de Appliance de Segurança de Rede, com assistência técnica por 12 meses, para atender as necessidades com a proteção dos equipamentos e das informações da Autarquia, em conformidade com o Edital de Pregão Eletrônico nº _____/2018 e seus Anexos.
ADVOGADOS: (*) _____

Na qualidade de Contratante e Contratado, respectivamente, do Termo acima identificado, e, cientes do seu encaminhamento ao TRIBUNAL DE CONTAS DO ESTADO, para fins de instrução e julgamento, damo-nos por CIENTES e NOTIFICADOS para acompanhar todos os atos da tramitação processual, até julgamento final e sua publicação e, se for o caso e de nosso interesse, para, nos prazos e nas formas legais e regimentais, exercer o direito da defesa, interpor recursos e o mais que couber.

Outrossim, estamos CIENTES, doravante, de que 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, de conformidade com o artigo 90 da Lei Complementar Estadual n° 709, de 14 de janeiro de 1993, precedidos de mensagem eletrônica aos interessados.

São Carlos, _____ de _____ de 2018.

CONTRATANTE:

Nome e cargo:

E-mail institucional
E-mail pessoal:
Assinatura: _____

CONTRATADA:

Nome e cargo:
E-mail institucional:
E-mail pessoal:
Assinatura: _____

(*) Facultativo. Indicar quando já constituído.

ANEXO VII

TERMO DE REFERÊNCIA

PARA AQUISIÇÃO DE NEXT GENERATION FIREWALL, ACCESS POINT WIFI, LICENÇAS, INSTALAÇÃO, TREINAMENTO E SUPORTE TÉCNICO.

1. INTRODUÇÃO

1.1. Contratação para aquisição e serviços especializados em processos e tecnologia da Informação (TI) nas atividades de segurança da informação com serviços para solução completa de NFGW / UTM para 300 (trezentos) usuários com fornecimento de Appliances NFGWs, Acess Point (AP WiFi), serviços, licenças, migração, treinamento, suporte técnico por 12 (doze) meses e ajustes estruturais na rede de dados do CONTRATANTE conforme as especificações técnicas a seguir.

1.2. A atual estrutura do CONTRATANTE prevê, a partir desta data, um crescimento mínimo de 50 usuários adicionais em até 3 (três) anos, totalizando 350 (trezentos e cinquenta) usuários conectados simultaneamente.

2. CONCEITOS

2.1. FIREWALL (NGFW / UTM) - protege redes de empresas com controles de segurança de alto desempenho, que fazem uso da inteligência fornecida pelas atualizações em tempo real pelo fabricante. Isso permite oferecer prevenção contra invasões, associadas a proteções completas de firewall de próxima geração, onde for necessário: em locais remotos, escritórios de filiais, data centers e na borda da rede. A Solução Next Generation Firewall prevê uma base sólida de proteções, incluindo controle granular de aplicativos, sistema de prevenção de intrusões (IPS), rede privada virtual (VPN) e inspeção detalhada de pacotes de rede, em um projeto unificado, eficiente e expansível. Sólidas tecnologias Anti-Invasão que decodificam e normalizam o tráfego de rede antes da inspeção e em todas as camadas de protocolo, expondo e bloqueando os mais avançados métodos de ataque.

2.2. UNIFIED THREAT MANAGEMENT (UTM) - na tradução literal para o português "Gerenciamento Unificado de Ameaças", é uma solução abrangente, criada para o setor de segurança de redes, vem ganhando notoriedade e se tornou a solução mais procurada na defesa das organizações. O UTM é teoricamente uma evolução do firewall tradicional, unindo a execução de várias funções de segurança em um único dispositivo: firewall,

prevenção de intrusões de rede, antivírus, VPN, filtragem de conteúdo, balanceamento de carga e geração de relatórios informativos e gerenciais sobre a rede.

2.3. ACCESS POINT OU AP - Ponto de Acesso é um dispositivo em uma rede sem fio que realiza a interconexão entre todos os dispositivos móveis. Em geral se conecta a uma rede cabeada servindo de ponto de acesso sem fio para outra rede, por exemplo, a Internet. Vários pontos de acesso podem trabalhar em conjunto para prover um acesso em uma área maior. Esta área é subdividida em áreas menores, sendo cada uma delas coberta por um ponto de acesso, provendo acesso sem interrupções ao se movimentar entre as áreas através de roaming.

2.4. IPS - é um sistema de prevenção de intrusão com tecnologia de segurança/prevenção de ameaças que, automaticamente, examina os fluxos de tráfego de rede para detectar e prevenir exploits de vulnerabilidade. Os exploits de vulnerabilidade geralmente vêm na forma de entradas com códigos maliciosos em aplicativos ou serviços estratégicos que os invasores usam para interromper e obter o controle sobre um aplicativo, uma rede ou máquina. Depois de um exploit bem-sucedido, o invasor pode desabilitar o aplicativo alvo (resultando em um estado de negação de serviço) ou pode acessar todos os direitos e autorizações disponíveis para o aplicativo comprometido.

2.5. CONTROLE DE APLICAÇÃO - Além dos recursos citados, o controle baseado em aplicação, ou filtro de camada 7 (Modelo OSI), apresenta uma grande vantagem no gerenciamento de segurança da informação nos dias atuais, onde cada vez menos as políticas baseadas em portas, protocolos e endereços são efetivas. O controle de aplicação filtra o conteúdo da última camada de um pacote de rede, a fim de identificar, independente de endereço, porta e protocolo, o comportamento das aplicações, e com base nisso e na política configurada, permite ou bloqueia o acesso. Através de uma base de conhecimento do comportamento das aplicações, os fornecedores oferecem atualizações regulares (como ocorre com vacinas de antivírus) para garantir que a eficiência do controle permaneça mesmo depois de atualizações das aplicações, como Skype, TorBrowser, BitTorrent e outros.

2.6. FILTRO DE CONTEÚDO WEB - ferramenta que verificará e encerrará qualquer tipo de conexão insegura que um dispositivo tentará fazer utilizando a rede corporativa da empresa. Além de verificar o nome do domínio acessado, o filtro analisará todo o tráfego web, permitindo que somente conteúdos seguros sejam exibidos na tela do computador do usuário. Dessa forma, a empresa terá mais confiança nos dados que são transmitidos pela

sua rede e os seus colaboradores terão acesso a conteúdo seguro e livre de códigos maliciosos. Geralmente esta função cabe ao NGFW, entretanto alguns antivírus possuem esta mesma funcionalidade, mas de forma não gerenciada ou centralizada no NFGW. A análise de conteúdo unificada inclui análise de ameaças em tempo real, de forma unificada oferece diversos benefícios. Primeiro, a liberdade para implementar soluções de segurança de conteúdo na nuvem ou localmente oferecendo a flexibilidade para cumprir os requisitos de segurança com a administração unificada em uma única central.

2.7. SEGURANÇA DE BORDA - tem como objetivo proteger a rede interna de invasões vindas da internet, controlar a navegação com relatórios e controle do tráfego (portas TCP/IP) tanto de dentro da rede local para internet quanto da internet para a rede local, garantindo mais segurança e integridade das informações, servidores, dispositivos e computadores da empresa. Com a segurança de borda estes ataques podem ser prevenidos. Atualmente existem vários tipos de segurança de borda, que vão desde a mais básica controlando apenas o tráfego de entrada e saída da internet até a mais avançada, equipada com sistema de segurança, capaz de interceptar e impedir ataques hacker.

2.8. PROTEÇÃO APT - (Advanced Persistent Threats, ou APTs) tem como foco a análise de comportamento para determinar se um arquivo é malicioso. O APT identifica e envia arquivos suspeitos para um simulador baseado em nuvem, um ambiente virtual em que o código é analisado, emulado e executado para determinar o potencial de ameaça. Ameaças avançadas, incluindo ameaças persistentes avançadas. São projetadas para reconhecer métodos de detecção e permanecerem ocultas. O APT oferece o nível mais profundo de visibilidade sobre comportamento de pragas virtuais e é também o mais difícil de ser detectado.

2.9. SANDBOX - são soluções adicionais de "próxima geração" para lidar com ameaças desconhecidas. A Sandbox é um ambiente seguro isolado, que imita um sistema de computador inteiro. Na Sandbox, programas suspeitos podem ser executados para monitorar seu comportamento e compreender a sua finalidade, sem pôr em perigo a rede de uma organização.

2.10. CRYPTO-RANSOMWARE - Ransomware é um tipo de software nocivo que restringe o acesso ao sistema infectado e cobra um resgate para que o acesso possa ser restabelecido, caso não ocorra, os arquivos podem ser perdidos e até mesmo publicados.

2.11. APPLIANCE - Dispositivo de hardware separado e dedicado com software integrado + firmware.

3. OBJETIVOS

3.1. Contratação para aquisição de equipamentos e serviços especializados nas atividades de segurança de tecnologia da Informação (TI) com fornecimento de serviços para NFGW / UTM Appliances NFGWs, Acess Point (AP WiFi), licenças e atualizações de subscrições por 12 meses ou mais, suporte técnico por 12 (doze) meses, migração, treinamento e ajustes estruturais na rede de dados da SAAE - SERVIÇO AUTÔNOMO DE ÁGUA E ESGOTO DE SÃO CARLOS, conforme as Especificações Técnicas a seguir:

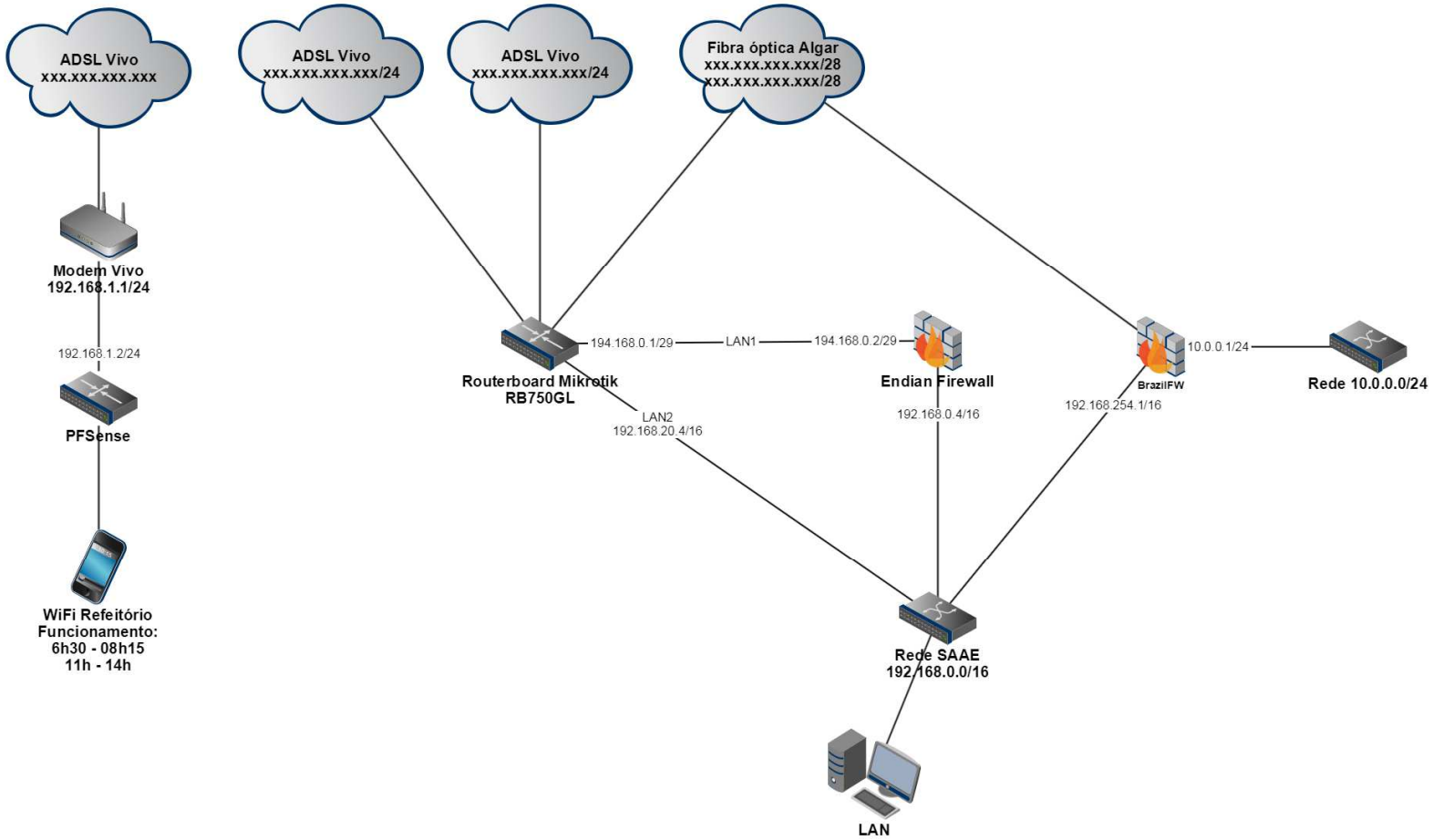
QUANT.	EQUIPAMENTO	LICENCIAMENTOS
1 UN.	NFGW / UTM, conforme especificações neste Termo.	Licenciamento e subscrição de aplicações de subscrições de segurança por 12 meses ou mais de atualizações e suporte do fabricante/fornecedor.
1 UN.	Servidor físico para registro e armazenamento de LOG´s de usuários, conforme especificações neste Termo.	Licenciamentos e subscrições de aplicações de gerenciamento e geração de relatórios com 12 meses de atualizações e suporte do fabricante/fornecedor.
1 UN.	Ponto de acesso sem fio (AP WiFi), conforme especificações neste Termo.	Licenciamento e subscrição de aplicações de gerenciamento com 12 meses ou mais de atualizações e suporte do fabricante/fornecedor.

Tabela1: Appliance NFGW com subscrições, AP WiFi e licenças.

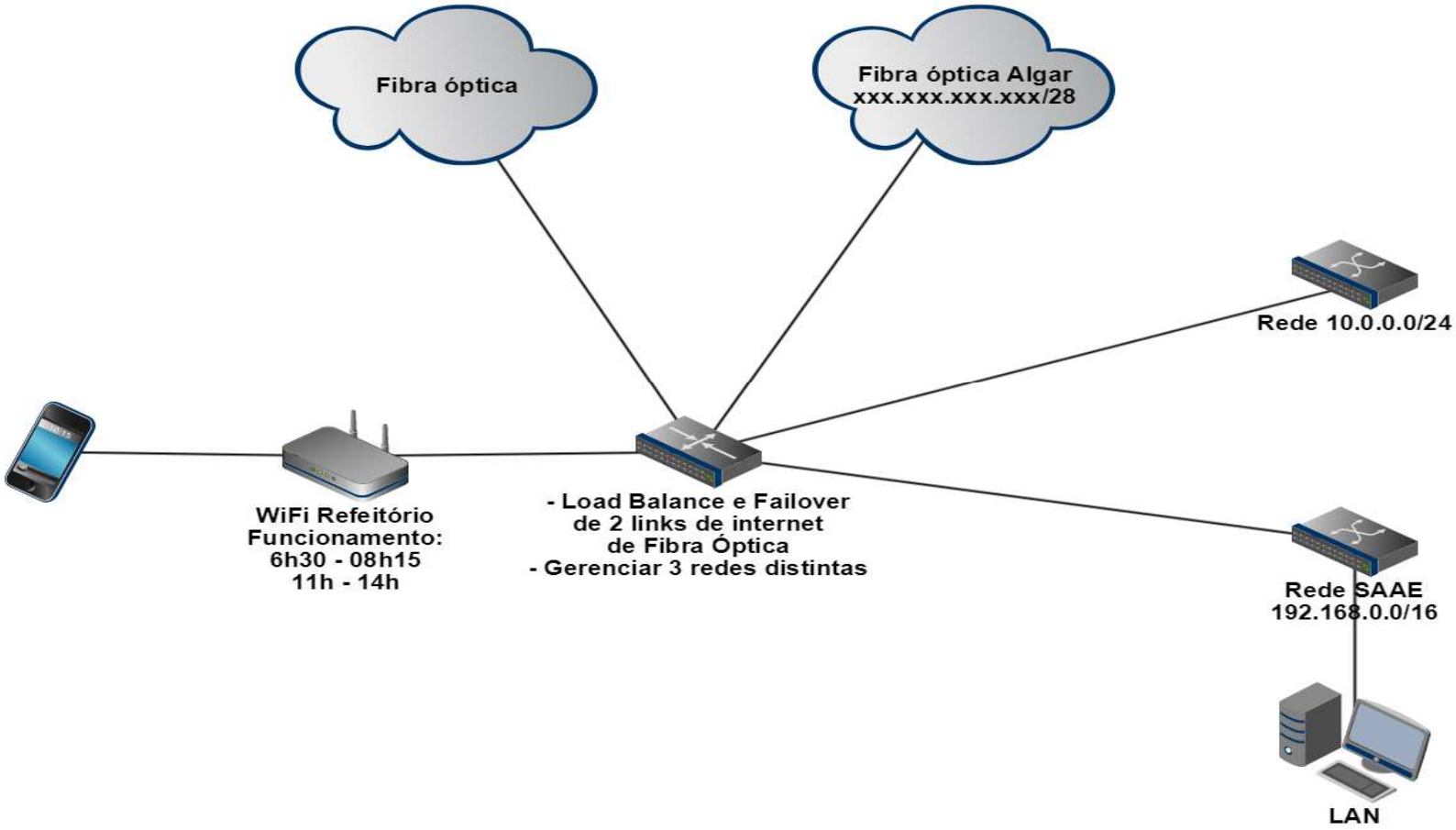
4. CENÁRIO ATUAL

4.1. Atualmente o SAAE – SERVIÇO AUTÔNOMO DE ÁGUA E ESGOTO DE SÃO CARLOS possui instalados dois servidores baseados em Linux – GNU em produção.

4.2. DIAGRAMA MACRO ATUAL



4.3. CENÁRIO MACRO PROPOSTO



5. DESCRIÇÃO DO LICENCIAMENTO

5.1. LICENÇAS DE USO – SUBSCRIÇÃO DE SEGURANÇA

5.1.1. Fornecimento de licença de uso de todos os serviços e aplicações baseados em subscrição de toda a solução de segurança proposta, atualização, suporte ao objeto deste projeto por um período mínimo de 12 (doze) meses e permitir a possibilidade de renovação das mesmas após seu período de vencimento.

5.2. Prazo de licenciamento mínimo será de 12 (doze) meses após a data de ativação das licenças especificadas em tabela a seguir:

CARACTERÍSTICAS – TIPO	INCLUSO	
Suporte LiveSecurity Service	Sim	**PRAZO: 12 (DOZE) OU MAIS MESES**
Controle de Aplicação	Sim	
Gateway AntiVirus (AV)	Sim	
Intrusion Prevention (IPS)	Sim	
Reputation	Sim	
Spams	Sim	
WebS	Sim	
APT	Sim	
Sandbox	Sim	
Suporte e manutenção AP WiFi	Sim	
Suporte e manutenção Server LOG´s	Sim	
DLP	Sim	

Tabela 2 – Licenças

5.3. Possuir licenças capazes de habilitar os recursos de filtro de conteúdo e gateway, crypto-ransomware, antivírus, antispyware descritas nas características do NFGW.

5.4. Deverão permitir atualização, contínua, gratuita e automática. Estão inclusos os serviços de instalação das licenças e configuração dos equipamentos, bem como serviços de suporte constantes no edital.

5.5. As licenças deverão ser autossuficientes para cada aquisição, isto é, devem permitir a habilitação dos recursos sem que haja necessidade de novas aquisições.

5.6. As licenças de todas as aplicações propostas deverão ser válidas por um prazo mínimo de 12 meses, renováveis sem custos para a CONTRATANTE por igual período ou mais.

6. DESCRIÇÃO TÉCNICA DETALHADA DO NGFW – UTM

6.1. Fornecimento, implantação e configuração de solução se segurança de redes atualizada, 100 % nova e de 1º uso com todas as licenças de uso necessárias incluindo todos os serviços baseados em subscrição, de toda a solução de segurança objeto deste projeto permitindo a possibilidade de renovação das mesmas após seu período de vencimento.

6.2. Firewall Appliance NFGW para instalação em Rack 19" máximo 2U´s, baseado na tecnologia Stateful Inspection na inspeção de todas as 7 camadas do modelo OSI, com funcionalidade de operação e licença de IDS/IPS inclusas no fornecimento. Não são aceitas soluções baseadas em servidores de terceiros.

6.3. Firewall Appliance NFGW - UTM com hardware dedicado, desenvolvido, fabricado, certificado e homologado pelo mesmo fabricante da solução/software.

6.4. Não serão aceitos Appliances de marcas, fabricantes ou fornecedores diferentes.

6.5. As soluções propostas devem ser comprovadamente atuais e constar na relação de produtos e serviços do fabricante/distribuidor da solução. Não serão aceitas soluções obsoletas, já fora de linha de produção ou mesmo descontinuadas. A comprovação do item obrigatoriamente será feita no ato de apresentação da proposta.

6.6. O equipamento é do tipo Appliance (dispositivo de hardware separado e dedicado com software integrado + firmware), com suporte à proteção imediata contra ameaças (default threat protection / zero day threat protection), Filtro de Conteúdo, IPS, Anti-spam, Anti-virus, Anti crypto-ransomware, Autoridade de Reputação na Web, Controle de Aplicações e APT.

6.7. O equipamento deve oferecer suporte à no mínimo três zonas de segurança: zona externa, privada e opcional (DMZ).

6.8. O equipamento deve oferecer suporte à configuração de endereços IP estáticos e dinâmicos (por DHCP e PPPoE) em interfaces externas.

6.9. O tráfego de firewall (firewall throughput) deve suportar 4,0 Gbps ou mais de tráfego de firewall.

6.10. Tráfego do NFGW (throughput): o equipamento deve suportar 0,8 Gbps de vazão de NFGW ou mais.

6.11. Conexões concorrentes (bi-direcionais): o equipamento deve suportar 3.000.000 conexões concorrentes bidirecionais ou mais.

6.12. O equipamento deve oferecer suporte a regras de firewall com autenticação de usuários (sem limites de número de usuários) a partir de base de dados interna e servidores de autenticação RADIUS, SecureID, LDAP e Active Directory.

6.13. O equipamento deve oferecer suporte a serviço de DNS dinâmico (Dynamic DNS) no caso de interfaces externas serem configuradas com endereços IP dinâmicos.

6.14. A solução proposta utilizará dispositivos de armazenamento de dados de qualidade, adequados e compatíveis objetivando minimizar a possibilidade de falhas.

6.15. O sistema deve oferecer suporte à implementação de regras de firewall de tipo Proxy (em camada 7 ou camada de aplicação) para os seguintes protocolos: HTTP, HTTPS, POP3, SMTP, FTP, DNS, VoIP (H.323 e SIP) e TCP-UDP.

6.16. As regras de firewall de tipo Proxy para protocolo HTTP devem permitir controlar, no mínimo, os seguintes aspectos do protocolo:

- HTTP Request: General Settings (Configurações Gerais);
- HTTP Request: Request Methods (Métodos HTTP);
- HTTP Request: URL Paths (URLs);
- HTTP Request: Header Fields (Campos de Header);
- HTTP Request: Authorization (Autorização);
- HTTP Response: General Settings (Configurações Gerais);
- HTTP Response: Header Fields (Campos de Header);
- HTTP Response: Content Types (Tipos MIME);
- HTTP Response: Cookies (Cookies);
- HTTP Response: Body Content Types (Tipos de Arquivos);
- Use a Caching Proxy Server (Uso de Servidor de Cache);
- Exceptions (Exceções);
- Safe Search Enforcement (Suporte a Busca Segura);
- Web Filter (Filtro de Conteúdo);
- AntiVirus (Anti-virus);

- Reputation Enabled Defense (Defesa por Autoridade de Reputação);
- Deny Message (Mensagem de Bloqueio);
- Proxy and AV Alarms (Geração de Alarmes).

6.17. As regras de firewall de tipo Proxy para protocolo HTTPS devem permitir controlar, no mínimo, os seguintes aspectos do protocolo:

- General Settings (Configurações Gerais);
- Content Inspection (Inspeção de Conteúdo);
- Bypass List (Lista de Bypass);
- WEB_FILTRO (Filtro de Conteúdo);
- Certificate Names (Certificados Digitais);
- Proxy and AV Alarms (Geração de Alarmes).

6.18. As regras de firewall de tipo Proxy para protocolo POP3 devem permitir controlar, no mínimo, os seguintes aspectos do protocolo:

- General Settings (Configurações Gerais);
- Authentication (Autenticação);
- Content Types (Tipos MIME);
- File Names (Nomes de Arquivos);
- Headers (Headers);
- Deny Message (Mensagem de Bloqueio);
- AntiVirus (Anti-virus);
- Proxy and AV Alarms (Geração de Alarmes).

6.19. As regras de firewall de tipo proxy para protocolo SMTP devem permitir controlar, no mínimo, os seguintes aspectos do protocolo:

- General Settings (Configurações Gerais);
- Greeting Rules (Regras do Protocolo);
- ESMTP Settings (Configurações de ESMTP);
- TLS Encryption (Criptografia via TLS);
- Authentication (Autenticação);
- Content Types (Tipos MIME);
- File Names (Nomes de Arquivos);
- Mail From / Rcpt To (Origem / Destino);
- Headers (Headers);
- AntiVirus (Anti-virus);
- Deny Message (Mensagem de Bloqueio);

- Proxy and AV Alarms (Geração de Alarmes).

6.20. As regras de firewall de tipo proxy para protocolo FTP devem permitir controlar, no mínimo, os seguintes aspectos do protocolo:

- General Settings (Configurações Gerais);
- Commands (Comandos);
- Content – Upload (Upload de Arquivos);
- Content – Download (Downoad de Arquivos);
- AntiVirus (Anti-virus);
- Proxy and AV Alarms (Geração de Alarmes).

6.21. As regras de firewall de tipo proxy para protocolo DNS devem permitir controlar, no mínimo, os seguintes aspectos do protocolo:

- General Settings (Configurações Gerais);
- Opcodes (Códigos de Operação);
- Query Types (Tipos de Consulta DNS);
- Query Names (Nomes de Consulta DNS);
- Proxy and AV Alarms (Alarmes);
- As regras de firewall de tipo proxy / application layer gateway para protocolo H.323 devem permitir controlar, no mínimo, os seguintes aspectos do protocolo:
- General Settings (Configurações Gerais);
- Access Control (Controle de Acesso);
- Denied Codecs (Codecs Bloqueados).

6.22. As regras de firewall de tipo proxy / application layer gateway para protocolo SIP devem permitir controlar, no mínimo, os seguintes aspectos do protocolo:

- General Settings (Configurações Gerais);
- Access Control (Controle de Acesso);
- Denied Codecs (Codecs Bloqueados).

6.23. O equipamento deve suportar 45.000 novas conexões por segundo.

6.24. Suporte a VPNs (Virtual Private Networks – Client/Server).

6.25. Vazão de VPN (VPN throughput): o equipamento deve suportar 2,0 Gbps de vazão de VPN.

6.26. A solução deve oferecer suporte a VPNs Móveis (Usuário – Equipamento) sobre protocolos IPSec, SSL e PPTP.

6.27. Deve incluir no mínimo licenciamento para 100 usuários móveis usando protocolo IPSec.

6.28. Deve incluir no mínimo licenciamento para 100 usuários móveis usando protocolo SSL.

6.29. Deve suportar no mínimo 75 VPNs fixas (Equipamento – Equipamento ou entre localidades) usando protocolo IPSec.

6.30. O equipamento deverá suportar a configuração de VPNs fixas com qualquer outro produto que ofereça suporte ao padrão IPSec.

6.31. Os seguintes mecanismos de autenticação devem ser suportados pela solução: DES, 3DES, AES 128-, 192-, 256-bit.

6.32. Os seguintes mecanismos de encriptação devem ser suportados pela solução: SHA-1, MD5, IKE Pre-Shared Key, certificados digitais.

6.33. Deve oferecer suporte a Dead Peer Detection (DPD).

6.34. Deve oferecer suporte a VPN Failover.

6.35. Deve oferecer suporte a tráfego de broadcast e multicast sobre VPNs.

6.36. O equipamento deverá poder suportar funcionalidades de Filtro de Conteúdo via subscrição adicional, renovável anualmente, sem a necessidade de equipamento dedicado.

6.37. As funcionalidades de Filtro de Conteúdo devem incluir a opção de filtro por categorias, devendo contar com um mínimo de 50 categorias.

6.38. As funcionalidades de Filtro de Conteúdo poderão ser configuradas glandularmente por usuário, grupo de usuários, endereço IP, grupo de endereços IP, sub-redes e horários específicos, devendo contar com um mínimo de 50 categorias.

6.39. A solução deve permitir estabelecer exceções quanto ao Filtro de Conteúdo, tanto no sentido de permissão (allow) quanto de bloqueio (deny).

6.40. A solução deve permitir filtrar conteúdo em múltiplos idiomas.

6.41. A funcionalidade de Filtro de Conteúdo deverá possibilitar a consulta a uma base de dados local (sobre interfaces privadas ou opcionais – DMZ), além da possibilidade de consultar uma base de dados externa.

6.42. A solução de Filtro de Conteúdo deverá suportar, no mínimo, os protocolos HTTP e HTTPS.

6.43. A solução de Filtro de Conteúdo deverá suportar recursos on-line que possibilitem solicitar a inclusão, exclusão ou mudança de classificação de novos sites ou sites existentes.

6.44. A base de dados local deverá suportar atualização automática. O filtro de Conteúdo exige que o administrador inicialmente classifique os websites no banco de dados. Informações serão on-line. A base de dados do Filtro de Conteúdo deverá ser mantida por um ou mais fabricantes listados no quadrante do Gartner para URL Filtering.

6.45. A solução deve permitir suportar a descompressão de arquivos comprimidos pelos algoritmos mais comuns (formatos .rar, .tar, .tgz, .gz, .zip, .gzip, .jar, .chm, .lha, .pdf, container XML/HTML, container OLE – documentos do Microsoft Office, .cab, .arj, .ace, .bz2 – Bzip e .swf) no mínimo de 4 níveis.

7. SOLUÇÃO DE ANTIVÍRUS INCLUSA

7.1. O equipamento suportará funcionalidades de serviço de Antivírus via subscrição adicional, renovável anualmente, sem a necessidade de equipamento (box) dedicado.

7.2. A atualização das assinaturas da solução de Antivírus deverá ser programável e automática, havendo adicionalmente a possibilidade de atualização de forma manual, a critério do administrador.

7.3. A solução de Antivírus deverá suportar serviços de quarentena, remoção de arquivos infectados, bloqueio de conexão (drop) e bloqueio de endereços (block).

7.4. O "engine" de verificação de código hostil utilizada pela solução de Antivírus será fornecido por empresa reconhecida por sua especialização no assunto.

7.5. A solução de antivírus proposta deverá suportar a detecção e bloqueio de código hostil em geral, incluindo vírus, cavalos de Tróia (trojans), vermes (worms), spyware e rogueware.

7.6. A solução de antivírus deverá suportar os protocolos HTTP, HTTPS, FTP, SMTP, TCP-UDP e POP3.

7.7. As assinaturas de antivírus devem ser fornecidas por um ou mais fabricantes listados no Gartner para Antivírus.

7.8. Vazão de Antivírus (AV throughput): o equipamento deve suportar 1,2 Gbps ou mais de tráfego.

7.9. A solução, os licenciamentos e os subscriptions, durante o período contratual, deve prover identificação, monitoramento e proteção contra Crypto-Ransomwares e todas as variações de encriptadores de arquivos e pragas virtuais similares.

8. SOLUÇÃO DE SANDBOX

8.1. A solução de sandbox deve possuir emulação de javaScript ou outra tecnologia similar em tempo real e análise comportamental.

8.2. A solução deve criar, para cada ameaça, um relatório profundo de análise forense, com correlação de evidências e priorização de APT, realizando uma pré-filtrarem do tráfego e somente submetendo para análise do sandbox arquivos suspeitos, garantindo assim uma menor latência e impacto para o usuário final.

8.3. Deve possuir defesas atualizadas contra Ransomware, APT (Advanced Persistent Threat), malwares desconhecidos e ataques direcionados, detectando, bloqueando e respondendo contra ameaças utilizando tecnologia sandbox baseada em nuvem.

8.4. Deve criar para cada ameaça um relatório profundo de análise forense, com correlação de evidências e priorização de APT, realizando uma pré-filtrarem do tráfego e somente submetendo para análise do sandbox arquivos suspeitos, garantindo assim uma menor

latência e impacto para o usuário final.

8.5. Caso o hash do arquivo nunca tenha sido analisado previamente, uma cópia do arquivo suspeito deve ser submetida ao sandbox. O arquivo deve ser então aberto na nuvem e todo o comportamento causado deve ser monitorado e analisado, resultando assim na liberação deste arquivo para o usuário ou seu bloqueio.

8.7. A solução proposta deve possuir proteção contra malwares avançados e ameaças de dia zero. O APT tem como foco a análise de comportamento para determinar se um arquivo é malicioso. O APT identifica e envia arquivos suspeitos para um simulador de última geração baseado em nuvem, um ambiente virtual em que o código malicioso é analisado, emulado e executado para determinar o potencial de ameaça e consequentemente bloqueá-la.

9. SOLUÇÃO DE IPS

9.1. O equipamento deverá poder suportar funcionalidades de serviços de IPS via subscrição adicional, renovável anualmente, sem a necessidade de equipamento (box) dedicado.

9.2. A atualização das assinaturas de ataques utilizadas pela solução de IPS deverá ser programável e automática, havendo adicionalmente a possibilidade de atualização de forma manual, a critério do administrador.

9.3. A solução de IPS deverá permitir a classificação das ameaças por nível de risco / severidade dos ataques, com não menos de 5 (cinco) níveis com a geração de alarmes e registros de log.

9.4. A solução de IPS deverá suportar ações de bloqueio de conexão (drop) e de bloqueio de endereços fonte de ataques (block), bem como a geração de alarmes por nível de risco.

9.5. A solução de IPS deverá suportar a detecção de ameaças em todos os protocolos e portas, independente do tipo de regra de firewall utilizada.

9.6. A solução de IPS deverá suportar a configuração de exceções quanto à análise de tráfego de rede por assinaturas de ataques.

9.7. A solução de IPS deverá oferecer um portal, acessível via Internet, na forma de uma base de dados onde possam ser obtidas informações adicionais sobre as assinaturas de ataques utilizadas na detecção de ameaças.

9.8. A solução de IPS deverá suportar por default (default threat protection), proteção imediata contra ataques e ameaças do tipo ataques de inundação (SYN flood attacks, IPSec flood attacks, IKE flood attacks, ICMP flood attacks, UDP flood attacks), ataques de falsificação (spoofing attacks), ataques de varredura de portas e endereços (port / address space probes) e ataques de negação de serviços (DoS) / negação de serviços distribuída (DdoS).

9.9. Devem ser configuráveis, pelo administrador da solução, os limites para a detecção de ataques de inundação (flood) e de ataques de negação de serviços (DoS / DdoS).

9.10. Vazão de IPS (IPS throughput): o equipamento deve suportar 2,5 Gbps de vazão de IPS.

9.11. O equipamento deverá suportar serviços de NAT nas seguintes modalidades:

- NAT estático;
- NAT dinâmico;
- NAT 1-to-1;
- IPSec NAT Tranversal;
- NAT sobre VPN (1-to-1 NAT Through VPN);
- NAT baseado em políticas (Policy-Based Dynamic NAT).

9.12. O equipamento deverá suportar serviços de PAT (Port Address Translation).

10. INTERFACES WAN/LAN/ RS232

10.1. O equipamento deverá oferecer suporte à divisão de cargas entre servidores (server load-balance) instalados no CONTRATANTE atualmente para 2 (dois) links fibra óptica 10MB full – Algar e VIVO.

10.2. O equipamento suportará um número mínimo de 8 (oito) interfaces 10/100/1000Mbps, (RJ45) as quais devem poder ser configuradas em qualquer das zonas de segurança disponíveis, a saber, zona externa, privada ou opcional (DMZ), bem como interfaces de gerência. Todas as portas Ethernet devem estar na parte da frente do

dispositivo.

10.3. O equipamento deverá suportar no mínimo 1 (uma) interface de gerência no padrão serial RS232 RJ45 ou DB9 e 2 (duas) ou mais interfaces USB.

10.4. O equipamento deverá oferecer serviços de multi-wan (suporte a múltiplos links / enlaces externos), com suporte a no mínimo quatro interfaces destinadas à zona externa de segurança, com possibilidade de funcionamento em modo fail-over ou em modo de divisão de carga (load-balancing), neste caso com possibilidade de definição pelo administrador do algoritmo a ser utilizado (round-robin, weighted round-robin, routing table ou interface overflow).

10.5. O equipamento deverá suportar, no mínimo, 75 VLANs (Virtual LAN´s).

10.6. O equipamento deverá suportar serviços de gerência de tráfego (traffic management) e de QoS (Quality of Services – qualidade de serviços).

10.7. O equipamento deve poder ser implementado em modo de roteador (modo routed), em modo semi-transparente (modo drop-in, com endereço IP único para todas as interfaces de rede) e em modo transparente (modo bridge ou switch).

10.8. O equipamento deve oferecer suporte a Ipv6 em conformidade com o Ipv6 Forum (Product Classification = Router; Ipv6 Ready Phase 2 – Gold Logo).

10.9. O equipamento deve suportar esta funcionalidade de serviços de Controle de Aplicações via subscrição adicional, renovável anualmente, sem a necessidade de equipamento (box) dedicado.

10.10. A atualização das assinaturas de aplicações utilizadas pela solução de Controle de Aplicações deverá ser programável e automática, havendo adicionalmente a possibilidade de atualização de forma manual, a critério do administrador.

10.11. A solução de controle de aplicações deverá oferecer um portal, acessível por Internet, na forma de uma base de dados onde possam ser obtidas informações adicionais sobre as aplicações passíveis de serem controladas.

11. AUTENTICAÇÕES DE USUÁRIO

11.1. A solução suportará as seguintes autenticações de usuário:

- Banco de dados interno;
- Windows Active Directory;
- LDAP e RADIUS;
- Captive portal configurável.

11.2. No caso do Active Directory, a solução deve fornecer uma opção "Single Sign-On" (SSO) para que os usuários não necessitem autenticar-se no firewall depois de terem autenticados no domínio AD.

11.3. Quando a Autenticação de Usuário é usada, os relatórios devem incluir o nome de usuário e endereço IP usado para fazer a conexão.

11.4. A solução deve ter a opção de redirecionamento dos usuários automaticamente para o portal de autenticação quando SSO não é utilizado.

11.5. O Portal de autenticação deve suportar usuários que se conectam a partir de dispositivos móveis, como smartphones.

11.6. A solução deverá permitir monitorar e desconectar usuários internos do equipamento, em tempo real e por espaço de tempo definido pelo administrador, sem necessidade de criação de regras ou políticas de segurança adicionais.

11.7. A solução deverá oferecer a possibilidade de visualização on-line de:

- Usuários autenticados (authentication list);
- Endereços IP bloqueados (blocked sites).

11.8. O equipamento deverá cumprir, ou estar em processo de cumprir, com as certificações de segurança eletrônica (ICSA Firewall, ICSA IPSec VPN, FIPS 140-2, Common Criteria EAL4+ e VPNC) no mínimo as listadas.

12. OUTRAS ESPSCIFICAÇÕES DA SOLUÇÃO

12.1. A solução deverá permitir a geração e envio de alarmes / notificações por protocolo SNMP v2 ou v3, janela de pop-up ou mensagem de e-mail.

12.2. A solução deverá suportar administração via interface web (browser), por interface de

rede, sobre protocolo seguro HTTPS.

12.3. A solução deverá permitir alterar o número da porta TCP usada para conexões HTTPS.

12.4. A solução deverá suportar administração via interface gráfica (sistema específico de gestão), por interface de rede, sobre protocolo HTTPS.

12.5. A solução deverá suportar recursos visualização de conexões simultâneas a partir de elementos de rede em quaisquer de suas interfaces de rede.

12.6. A solução deverá oferecer uma console que permita acompanhar em modo gráfico o desempenho do equipamento (performance console) em termos de informações do sistema (uso de CPU e memória), informações sobre as interfaces de rede e informações sobre as políticas e regras de segurança.

12.7. Deverão permitir a utilização por número indefinido de usuários ou endereços IP.

12.8. A ferramenta de gerenciamento e administração de firewall deve permitir configuração, acompanhamento e implementação centralizados, capaz de possibilitar aos administradores, definir, distribuir e implementar um amplo número de serviços, atualizações e política de segurança para os firewalls gerenciados pela solução.

12.9. A solução proposta deverá permitir o backup de configuração de sistemas (regras), aplicação de "Patches" e novas atualizações de softwares, gerenciamento de modificações e análise de logs.

12.10. A solução proposta deverá permitir a visão do status atual da solução de segurança, relatórios gráficos e atividades de rede por firewall.

12.11. A solução proposta deverá possibilitar monitoramento por análise de dados ou por falhas, incluindo status do firewall e dos túneis VPN em tempo real.

12.12. A solução proposta deverá permitir a visualização do gerenciamento e dos relatórios através de interfaces gráficas.

12.13. A solução proposta deverá possibilitar o envio de alertas e notificações por e-mail.

12.14. A solução proposta deverá permitir a configuração de mais de um perfil de administrador e suas respectivas permissões.

12.15. A solução proposta deverá permitir o gerenciamento centralizado de, no mínimo, 10 (dez) NFGWs no equipamento NGFW da unidade central.

12.16. Caso seja de outra marca a licitante deverá disponibilizar software ou Appliance para a realização do gerenciamento centralizado.

13. REGISTRO DE ATIVIDADE E LOGS

13.1. O sistema sendo oferecido deve permitir a implementação de servidor de registro de log´s de maneira a centralizar o armazenamento dos registros gerados pelo equipamento. A solução deverá, opcionalmente, suportar a configuração de múltiplos servidores de logs.

13.2. O licitante incluirá na proposta **1 (uma) unidade de servidor físico dedicado**, conforme o item 14 deste Termo.

13.3. O serviço de armazenamento de registros deve estar baseado em protocolo TCP/IP e utilizar SGBD (Sistema de Gerenciamento de Banco de Dados), licença a qual deverá estar incluída como parte integral da proposta, permitindo-se opcionalmente a utilização de uma base de dados compatível pré-existente.

13.4. O tamanho máximo da base de dados deve ser configurável pelo administrador, bem como configurar alertas a serem gerados quando o tamanho da base de dados alcançar o tamanho máximo definido.

13.5. A transmissão dos logs deve ser feita de maneira encriptada, sem que para tal se requeira a configuração de VPNs.

13.6. A solução deverá oferecer suporte à utilização opcional de serviços de logs de sistema (syslog) para armazenamento de logs.

13.7. A solução deverá suportar a geração de, ao menos, 50 (cinquenta) modelos diferentes de relatórios administrativos e de gerenciamento a partir de múltiplos servidores de logs.

13.8. O serviço de geração de relatórios deverá permitir gerar relatórios em formato PDF,

CSV e HTML.

13.9. O serviço de geração de relatórios deverá permitir automatizar a geração de relatórios.

13.10. A solução deverá oferecer acesso por um portal web para a visualização de relatórios.

13.11. A solução proposta deverá possibilitar a geração de notificações e log´s das tentativas de ataques;

13.12. A implantação do sistema operacional do servidor e do SGBD para o registro dos logs é de inteira responsabilidade da contratada. O backup dos dados é de responsabilidade da CONTRATANTE.

14. SERVIDOR FÍSICO PARA REGISTRO E ARMAZENAMENTO DE LOG´s INCLUSO

14.1. O CONTRATADO fornecerá, sem quaisquer custos adicionais, servidor físico dedicado para registro e armazenamento de log´s e aplicações para geração de relatórios.

14.2. O hardware proposto terá capacidade para registrar e armazenar o volume de dados gerado por 300 (trezentos) usuários, com capacidade mínima de armazenamento por 12 (doze) meses, totalmente compatível com o NGFW especificado.

14.3. O proponente deve prever todas as licenças legalizadas:

- Aplicações para gerenciamento e geração de relatórios;
- SGBD – Sistema de Gerenciamento de Banco de Dados;
- Sistemas Operacionais – Linux ou Windows.

14.4. O hardware do servidor proposto terá qualidade comprovadamente assegurada e será instalado em "rack 19". Deve ter no máximo 4U´s de altura, suporte e garantia total do fabricante/fornecedor, para todos os seus componentes, independente da solução de segurança proposta, de no mínimo de 12 (doze) meses.

14.5. O hardware do servidor proposto poderá ser integralizado, de marca/fabricante diferente da solução de segurança de rede proposta.

15. PONTO DE ACESSO SEM FIO

15.1. Incluso 1 (um) ponto de acesso sem fio (AP WiFi) da mesma marca do fabricante da solução, com ferramentas e aplicações de gerenciamento unificadas, para gerenciar os dispositivos AP e NGFW usando um único console, com as seguintes características técnicas:

- Recurso de filtragem de MAC;
- Relatórios de clientes;
- Tecnologia Captive Portal nativa;
- Autenticação 802.1X;
- Controle e segurança na WLAN;
- Instalação em ambiente interno / externo (classificação IP66);
- Frequência de operação do rádio selecionável - 2,4 GHz ou 5 GHz ;
- Faixas de frequência (GHz) 2,400 a 2,474 GHz, 5,150 a 5,250 GHz, 5,250 a 5,350 GHz, 5,470 a 5,725GHz, 5,725 a 5,850 GHz;
- Número de antenas: 2 internas, horizontal a 120 graus ou configuração similar;
- Ganho mínimo de antena: 6 (seis) dBi ou maior;
- Fluxos Tx/Rx: 2x2 MIMO com 2 fluxos espaciais ou configuração similar;
- Potência TX 20 dBm;
- Taxa de dados 300 Mbps ou maior;
- 8 (oito) SSID configuráveis;
- Configurações de Segurança: WPA-PSK, WPA2-PSK, WPA-PSK/WPA2-PSK (Misto), WPA-802.1X (Enterprise) WPA2-802.1X (Enterprise) WPA-802.1X/WPA2-802.1X (Misto) TKIP, AES, TKIP/AES, Captive Portal, lista de permissão/lista negra de MAC, TAG´s de VLAN;
- Interface Ethernet gigabit;
- Recursos de desempenho 802.11e WMM;
- Certificações Wireless: FCC, IC e CE;
- Segurança: NRTL/C, CB e CE;
- Controle de Substâncias Perigosas: RoHS;
- Adaptador CA e Injeção Power over Ethernet (PoE) incluso 802.3af/at ou injetor PoE compatível;
- Padrões IEEE suportados: 802.11a/b/g/n, 802.11i, 802.1q, 802.1X, 802.3af/at, 802.11e;
- Suporte e Manutenção: incluso licenças para 3 anos, suporte padrão para garantia de hardware, suporte técnico e atualizações;
- Acessórios e opções de montagem para parede e teto incluídos;
- TCO (Total Cost of Ownership) reduzido com gerenciamento simplificado do ciclo de vida do AP.

15.2. Visando a integração total da solução proposta, o aproveitamento de suas ferramentas e softwares de gerenciamento, não serão aceitos AP WiFi de fabricantes diferentes do NGFW - UTM.

16. DESCRIÇÃO DO SUPORTE TÉCNICO DURANTE A VIGENCIA DO CONTRATO E MIGRAÇÃO DO AMBIENTE

16.1. DESCRITIVO DOS SERVIÇOS DE SUPORTE NÍVEIS 1, 2 e 3

16.1.1. Os serviços de suporte técnico devem contemplar as seguintes ações e/ou premissas:

16.1.2. Chamados Nível 1 e 2 ilimitados tanto presenciais como remoto.

16.1.3. Chamados em regime de 8 x 5 conforme tabela SLA de severidades constantes da tabela de severidades abaixo:

NÍVEIS DE SEVERIDADE DOS CHAMADOS	
Nível	**Descrição**
1	Serviços totalmente indisponíveis.
2	Serviços parcialmente indisponíveis ou com degradação de tempo de resposta no acesso aos aplicativos.
3	Serviços disponíveis com ocorrência de alarmes, avisos, consultas sobre problemas, dúvidas gerais sobre o NFGW.

Tabela dos Prazos:

Tabela de Prazos de Atendimentos dos Serviços				
Modalidade	**Prazos**	**Níveis de Severidade**		
		1	**2**	**3**
On Site e telefone	Início de Atendimento	4 horas	6 horas	24 horas
	Término de Atendimento	8 horas	8 horas	72 horas
Telefone, e-mail e Web-helpdesk	Início de Atendimento	-	-	24 horas
	Término de Atendimento	-	-	144 horas

16.1.4. Atendimento (N1 e N2) para a Abertura de chamados e no fabricante Nível 3 (N3) com acompanhamento e aplicação da solução, atualizações, RMA (Garantia do FABRICANTE) se for o caso.

16.1.5. Acompanhamento, validações e atualizações e renovações a qualquer tempo mediante agenda e chamado.

16.1.6. Para os serviços de suporte técnicos, caberá a Licitante oferecer suporte técnico, em português, por profissional devidamente capacitado e certificado pelo fabricante, a Contratada deverá possuir Central de Atendimento disponibilizando contato por telefone, HelpDesk e e-mail em regime 8x5.

16.1.7. Recepcionar via telefone ou e-mail, e registrar corretamente à abertura de qualquer chamado técnico referente à solução.

16.1.8. Implantar e manter registros de atendimento adequados às necessidades de suporte técnico do CONTRATANTE.

16.1.9. Implantar e manter base de conhecimento adequada às necessidades específicas de suporte técnico do CONTRATANTE.

16.1.10. Solucionar problemas ou sanar dúvidas por telefone e/ou e-mail ou presencialmente (suporte local), quanto aos questionamentos repassados pela equipe do CONTRATANTE após abertura do chamado de acordo com a tabela de severidade.

16.1.11. Disponibilizar atualizações de softwares e firmwares dos produtos ofertados sem qualquer tipo de ônus para a CONTRATANTE, Garantia da solução proposta sem qualquer tipo de ônus, inclusive para substituição.

17. MANUTENÇÃO CORRETIVA OU PREVENTIVA

17.1. A CONTRATADA deve informar o CONTRATANTE, no prazo de até 10 (dez) dias uteis, sobre a disponibilização de atualizações de firmwares e ou softwares que compõem a solução e agendar a instalação dessas atualizações.

17.2. É de responsabilidade do CONTRATADO instalar, configurar e testar as atualizações necessárias para o bom funcionamento da solução, durante o prazo contratual.

17.3. Os agendamentos dessas atividades serão planejados juntamente com a CONTRATANTE e poderão ocorrer fora do horário de produção, caso seja necessário a parada dos equipamentos.

17.4. O CONTRATADO acompanhará os chamados desde sua abertura até seu encerramento, independente de existir ou não redirecionamento para outras equipes técnicas do próprio CONTRATADO ou do CONTRATANTE.

17.5. Quando solicitado pela CONTRATANTE serão gerados relatórios executivos mensais contendo as atividades realizadas e o resumo dos dados em aberto.

17.6. Os serviços de suporte técnico devem estar disponíveis em horário comercial durante sua vigência, de segunda a sexta-feira das 08:00h às 18:00h exceto feriados. Os chamados com nível de severidade críticos devem ser abertos e atendidos no regime (8x5) conforme a tabela de severidades.

17.7. Possibilitar a abertura de chamados diretamente com o fabricante da solução ou com seu representante credenciado e bem como o acesso ilimitado ao site do fabricante permitindo o download de atualizações, patchs de correção e documentações técnicas.

17.8. Caberá a Central de Atendimento da CONTRATADA ser o contato único entre a CONTRATADA e o CONTRATANTE registrando todos os chamados, solicitações e registros de ocorrência em sistema eletrônico específico para este, além de fornecer ao CONTRATANTE o número de chamado da ocorrência para acompanhamento.

17.9. Assistência total para resolução de falhas técnicas do NGFW, Servidor de LOG´s e AP WiFi e toda solução dentro dos prazos estabelecidos.

17.10. Orientação técnica e esclarecimento de dúvidas da equipe da CONTRATANTE.

17.11. Aplicação das regras e políticas do NGFW / UTM/ UTM (Segurança) e configuração do NFGW Application Control, Reputation, Web control, IPS e AV, APT, SANDBOX.

17.12. No ato de ativação dos sistemas a CONTRATADA atualizará o software para o release mais atual.

17.13. Acesso a console / serial e terminal de configuração para cada dispositivo;

17.14. Configuração de acesso administrativo usando HTTPS e SSH e verificação de DNS/NTP e conectividade básica de rede e roteamento;

17.15. Reconfiguração / ajustes do sistema básico de monitoramento (SYSLOG / configuração SNMP) e banco de dados;

17.16. Verificar se as funcionalidades do NGFW / UTM bem como as licenças ativas e suas configurações.

17.17. Prestação de serviços com fornecimento de licenças de uso de todos os serviços baseados em subscrição de toda a solução de segurança objeto deste projeto permitindo a possibilidade de renovação das mesmas após o período de vencimento.

17.18. A solução deve vir acompanhada de todos os acessórios, suportes, parafusos, cabos, conectores e demais itens necessários para a instalação e o imediato funcionamento do equipamento;

17.19. Deve vir acompanhado de manuais originais do fabricante e vir acompanhado de acessórios e do kit de suporte especifico para montagem.

17.20. A Contratada deverá executar a ativação da solução de Access Point ofertado aplicando as configurações em atendimento das necessidades da topologia a ser implementada no ambiente do CONTRATANTE.

17.21. Caberá a Contratada realizar a configuração completa do equipamento ofertado, e demais configurações necessárias para ativação da comunicação no ambiente, de acordo com a seguinte metodologia de trabalho:

17.22. Em até 5 (cinco) dias úteis, após a assinatura do contrato ou recebimento de termo análogo, o CONTRATADO agendará uma reunião preliminar com a equipe técnica do CONTRATANTE para definir o escopo e os prazos para realização dos serviços de instalação e configuração;

17.23. Deverá ser elaborado o plano de ativação contendo as configurações a serem aplicadas, contemplando as necessidades e particularidades do ambiente tecnológico do CONTRATANTE, para aprovação;

17.24. Configuração preliminar em ambiente de homologação, inclusive com atualização lógica que o NGFW / UTM possui para a última versão disponibilizada pelo respectivo fabricante;

17.25. Ativação no ambiente de produção conforme determinado no plano elaborado, incluindo sua configuração final para perfeito funcionamento;

17.26. A configuração do NGFW / UTM ofertado deve contemplar todos os aspectos e características disponíveis nos mesmos e seguindo o acordado em pré-projeto.

17.27. Os serviços serão realizados pela CONTRATADA na modalidade 8x5 (oito horas por dia, cinco dias na semana).

17.28. Serão permitidas manutenções remotas (corretivas e preventivas) previamente agendadas com o CONTRATANTE.

18. PRAZOS DA INSTALAÇÃO, MIGRAÇÃO E TREINAMENTO

18.1. A entrega da solução completa (materiais) deve ocorrer em até **30 (trinta) dias corridos** a partir da assinatura do contrato ou recebimento de termo análogo, no Almoxarifado da CONTRATANTE, situado na cidade de São Carlos – SP, Rua José Casale, nº 400, Jardim São Paulo, CEP 13570-450.

18.2. A instalação, configuração e migração das regras e serviços devem iniciar em até **15 (quinze) dias corridos** após a entrega da solução (itens 17.22 e 18.1). Deve ser efetuada de forma a não afetar o funcionamento dos sistemas, recursos ou equipamentos atualmente em operação e nem impedir ou interromper, por períodos prolongados, a rotina de trabalho dos colaboradores da CONTRATANTE.

18.3. Ao início do projeto, deverá ser convocada reunião da contratada com a equipe de tecnologia da CONTRATANTE.

18.4. Deverão ser apresentados os detalhes da solução contratada, bem como apresentados todos os aspectos de concepção do projeto, incluindo configurações e políticas.

18.5. Deverá ser apresentado pela CONTRATADA o plano de execução dos serviços, detalhando responsáveis, prazos e fases, além de previsão de eventos e seus impactos na

infraestrutura existente. Novas reuniões poderão ser convocadas por ambas as partes de modo a definir todos os pormenores da solução e eliminar pendências.

18.6. O serviço de migração deverá compreender a migração, adaptação e configuração necessária de todas as regras, redes, conexões, entre outros objetos e políticas existentes na CONTRATANTE. Atualmente, são adotadas as plataformas Linux / Windows e outros que deverão ser migrados para a nova solução.

18.7. Fará parte também do serviço de garantia e suporte técnico contratado, a garantia dos serviços prestados de implantação e migração das soluções.

18.8. No caso de necessidade de interrupção de sistemas corporativos, recursos, equipamentos ou das rotinas de trabalho de qualquer setor funcional em decorrência da instalação a ser efetuada, esta parada deverá ser devidamente planejada e acordada com antecedência junto à equipe técnica da CONTRATANTE.

18.9. Após a assinatura do contrato ou recebimento de termo análogo, os profissionais que executarão o serviço de implantação e migração deverão comprovar formalmente, através de declaração do fabricante da solução, certificados e certificações, conhecimento na solução oferecida.

18.10. É de obrigação do licitante revisar os documentos inicialmente submetidos no ato da homologação do vencedor ao qual incluem o planejamento, definição, detalhes de configuração da solução, cronograma de implantação e outras informações relevantes. Esse documento será aprovado pela equipe técnica do CONTRATANTE e servirá como referência para os serviços a serem executados.

18.11. O CONTRATADO, ao término da implantação e migração, entregará o caderno de documentação técnica do projeto, contendo todas as informações de configuração, testes, homologações, procedimentos de contingência e demais informações necessárias, para a operação e manutenção da solução;

18.12. Para cada compra adicional ou atualização significativa de firmware de NGFW - UTM, dentro do contrato estabelecido, estará incluso a atualização/treinamento para 2 (dois) técnicos da CONTRATANTE, e deverá ser ministrado por empresa certificada e autorizada pelo fabricante, nas dependências do CONTRATANTE ou, sendo viável, remotamente.

18.13. O treinamento será ministrado, por profissionais da CONTRATADA ou seu representante regional, dentro do município de São Carlos em ambiente próprio e dedicado para este fim.

18.14. Caso seja necessário treinamento fora deste município, a CONTRATADA é responsável pelas despesas de transporte, hospedagem e alimentação.

18.15. A carga horária necessária para conclusão do treinamento deve ser estabelecida pelo CONTRATADO e abrangerá todas as facilidades da solução adquirida incluindo administração de completa do firewall.

18.16. Materiais e apostilas impressas são de responsabilidade do CONTRATADO.

19. CONDIÇÕES GERAIS E VISITA TÉCNICA

19.1. O local da instalação do licenciamento tem como base as instalações de tecnologia do CONTRATANTE.

19.2. Todos os deslocamentos dos técnicos, bem como as obrigações trabalhistas, estadias, refeições, retiradas, devolução e instalações deverão correr por conta do CONTRATADO sob qualquer hipótese ou pretexto.

19.3. A contratada deverá apresentar declaração comprovando possuir condições para a instalação, configuração e acompanhamento do objeto deste edital.

19.4. O prazo de vigência do contrato será de 12 (doze) meses (mínimo) contados a partir da data de assinatura do mesmo.

19.5. O prazo mencionado no item anterior poderá ser prorrogado por igual (ais) e sucessivo (s) período (s), a critério unilateral do CONTRATANTE, até o limite legal, nos termos e condições permitidos pela lei nº 8.666/93.

19.6. Atestado de visita técnica, conforme **Anexo VIII**, comprovando o comparecimento do proponente aos locais onde serão instalados os equipamentos e ativados os licenciamentos, visando à verificação das condições e conhecimento do ambiente atual.

19.7. A visita acima mencionada deverá ser agendada com antecedência mínima de 24 (vinte e quatro) horas, pelo telefone (16) 3373-6420, solicitadas à GTI - Gerência de

Tecnologia da Informação.

19.8. A proponente deverá indicar antecipadamente o profissional responsável pela visita, razão social e CNPJ, por ocasião da visita, para que os mesmos sejam devidamente consignados no atestado de que trata este item.

19.9. Sendo facultada a visita técnica, o licitante que optar por não visitar os locais de instalação, atesta e confirma que entende e compreende toda e qualquer dificuldade técnica, operacional e logística oriunda da formulação de custos, elaboração das propostas, implantação, configuração, reconfiguração, manutenção, treinamento e suporte técnico na localidade especificada.

20. GARANTIAS

20.1. A garantia mínima para a solução de segurança de redes incluindo todos os materiais e serviços serão de no mínimo 12 (doze) meses, contados a partir da assinatura do contrato ou do recebimento de termo análogo.

20.2. Os serviços de manutenção preventiva e/ou corretiva serão prestados por representantes capacitados e oficiais da licitante vencedora, da qual o SAAE deverá ser informado quando for aberto um chamado para prestar o suporte técnico requisitado.

20.3. Acionada a garantia, em caso de defeitos que inviabilizem o uso ou reparo da solução, contempla a substituição completa do equipamento danificado ou seu conserto,

20.4. Todas as despesas de envio e recebimento do material, viagens e hospedagem de técnicos são de responsabilidade do CONTRATADO.

21. MEDIDAS ACAUTELADORAS

21.1. O CONTRATANTE, pautado em dispositivos legais poderá, sem a prévia manifestação do interessado, motivadamente, adotar providências acauteladoras, inclusive retendo o pagamento, em caso de não cumprimento das cláusulas contratuais.

22. SITUAÇÕES NÃO PREVISTAS NESTE TERMO DE REFERÊNCIA

22.1. Situações não previstas ou especificadas neste Termo de Referência serão tratadas

pontualmente, solucionadas pautando-se na Lei Federal nº 8.666, de 1993 e exclusivamente no interesse público do munícipio de São Carlos - SP.

22.2. Posteriormente à disputa e declarado o vencedor de certame, não serão aceitas mudanças significativas, adaptações, subcontratações, transferências de responsabilidades ou especificações fora do escopo estabelecido neste Termo de Referencia, salvo justificativa e posterior autorização do CONTRATANTE.

ANEXO VIII

MODELO DE ATESTADO DE VISITA TÉCNICA

Processo Licitatório nº: _____/2018.
Pregão Eletrônico nº: _____/2018.

Declaramos, para fins de participação na licitação em referência, que a empresa abaixo, qualificada, realizou visita técnica no local onde serão prestados os serviços, logo, tendo conhecimento do objeto desta licitação e ciência de todas as condições deste projeto.

São Carlos, _____ de _____ 2018.

_____
Responsável

Nome da Empresa: _____

CNPJ da Empresa: _____