



EDITAL

(Processo nº 51/2019)

MODALIDADE: PREGÃO Nº 07/2019
FORMA: PRESENCIAL
TIPO DE LICITAÇÃO: MENOR PREÇO
AQUISIÇÃO: GLOBAL

PREÂMBULO

A Presidente da Câmara Municipal de Vereadores de Santa Maria – RS (CMVSM), no uso de suas atribuições legais, determinou ao PREGOEIRO, designado através da Portaria nº 73/2019 (**Anexo X**), tornar público para conhecimento de quaisquer interessados, que, na data, horário e local a seguir indicados, será realizada Licitação na modalidade **PREGÃO PRESENCIAL**, do tipo de **MENOR PREÇO GLOBAL**, para **contratação de empresa capacitada para prestar serviço de solução para gerenciamento de conectividade de redes e prevenção de ameaças com suporte remoto para até 180 usuários**, conforme Termo de Referência (**Anexo II**). Este processo Licitatório prevê, no que se refere a todos os itens que compõem seu objeto, **participação exclusiva de Microempreendedores Individuais, Microempresas, Empresas de Pequeno Porte e outras que eventualmente venham a se enquadrar nos mesmos benefícios legais, conforme legislação vigente**. O presente processo licitatório obedecerá integralmente à Lei Federal nº 10.520, de 17 de julho de 2002, ao Decreto Municipal nº 072/2015, de 03 de agosto de 2015, que institui a modalidade Pregão no Município de Santa Maria, bem como às demais normas federais e municipais pertinentes ao assunto, no que couberem, em especial à Lei Federal nº 8.666/93, à Lei Complementar Federal nº 123/2006, com as alterações da Lei Complementar Federal nº 147/2014 e à Lei Municipal nº 5.245 de 05 de novembro de 2009.

1 – DO RECEBIMENTO E INÍCIO DA ABERTURA DOS ENVELOPES, PROPOSTA E DOCUMENTAÇÃO

LOCAL: Plenarinho da Câmara Municipal de Vereadores de Santa Maria, sito à Rua Vale Machado, nº 1415, Centro, CEP 97010-530, Santa Maria – RS.

DIA: 02/07/2019.

HORÁRIO: 14:00 HORAS.

1.1 Se no dia supracitado não houver expediente, o recebimento e o início da abertura dos envelopes referentes a este Pregão serão realizados no **primeiro dia útil** de funcionamento da Câmara Municipal de Vereadores de Santa Maria que se seguir, desde que não haja comunicação do Pregoeiro em contrário.

1.2 No local indicado serão realizados os procedimentos pertinentes a este Pregão, com respeito a:

1.2.1 credenciamento dos representantes;

1.2.2 consulta ao Cadastro Nacional de Empresas Inidôneas e Suspensas (**CEIS**) e ao Cadastro Nacional de Empresas Punidas (**CNEP**);

1.2.3 recebimento dos envelopes de proposta e documentação;

1.2.4 abertura dos envelopes de proposta dos licitantes;

1.2.5 abertura do envelope de documentação do licitante com proposta vencedora.

1.3 As decisões do Pregoeiro serão comunicadas mediante publicação na página *web*, no endereço www.camara-sm.rs.gov.br, com pelo menos **01 (um) dia de antecedência**, salvo com referência



àquelas que puderem ser comunicadas diretamente, mediante ofício, fac-símile ou outro similar, aos representantes legais dos licitantes, principalmente, quanto a:

- 1.3.1 habilitação ou inabilitação do licitante;
- 1.3.2 julgamento das propostas;
- 1.3.3 resultado de impugnação ou recurso porventura interposto;
- 1.3.4 resultado de julgamento deste Pregão.

1.4 A solicitação de esclarecimento de dúvidas a respeito das condições deste Edital e de outros assuntos relacionados a presente licitação deverá ser efetuada pelas empresas interessadas em participar do certame em até **02 (dois) dias úteis** que antecederem a data estabelecida no preâmbulo deste instrumento convocatório para a sessão de recebimento e abertura dos envelopes da Proposta e Documentação.

1.5 A resposta do Pregoeiro ao pedido de esclarecimento formulado será divulgada mediante publicação de nota na página *web* da Câmara Municipal de Vereadores de Santa Maria, no endereço www.camara-sm.rs.gov.br, menu "Licitações", cabendo aos interessados acessá-la.

2 - DO OBJETO

2.1 A presente licitação tem por objeto a contratação de empresa capacitada para prestar serviço de solução para gerenciamento de conectividade de redes e prevenção de ameaças com suporte remoto para até 180 usuários, conforme Termo de Referência (Anexo II), sendo sua aquisição do tipo **MENOR PREÇO GLOBAL**.

2.1.1 São partes integrantes deste objeto as demais condições e especificações diluídas neste Edital e seus anexos.

3 - DA PARTICIPAÇÃO NA LICITAÇÃO

3.1 Poderão participar deste Pregão quaisquer interessados que detenham atividade pertinente e compatível com o objeto, desde que, **EXCLUSIVAMENTE**, sejam **Microempreendedores Individuais, Microempresas, Empresas de Pequeno Porte e outras que eventualmente venham a se enquadrar nos mesmos benefícios legais, conforme legislação vigente**.

3.2 **NÃO** poderão participar deste Pregão as empresas que:

3.2.1 Encontrem-se em processo de falência, recuperação judicial, concurso de credores, dissolução ou liquidação;

3.2.2 Estejam cumprindo sanção de suspensão do direito de licitar ou de declaração de inidoneidade imposta pela Administração Pública, entendida esta como Administração Direta e Indireta da União, dos Estados, do Distrito Federal e dos Municípios, abrangendo inclusive as entidades com personalidade jurídica de direito privado, sob controle do Poder Público e das fundações por ele instituídas ou mantidas;

3.2.3 Constem no Cadastro Nacional de Empresas Inidôneas e Suspensas (**CEIS**) e no Cadastro Nacional de Empresas Punidas (**CNEP**), cujas consultas serão promovidas em atenção ao Ofício DCF nº 44/2017 do Tribunal de Contas do Rio Grande do Sul – TCE-RS, caso em que terão suas propostas integralmente desclassificadas;

3.2.4 Sejam reunidas em consórcio ou sejam controladas, coligadas ou subsidiárias entre si, ou ainda, qualquer que seja sua forma de constituição, quando estejam participando concomitantemente nos mesmos itens do processo licitatório;

3.2.5 Sejam estrangeiras e não funcionem regularmente no País;

3.2.6 Estejam proibidas por lei.



3.3 Os proponentes deverão ter pleno conhecimento dos termos deste edital e seus anexos, sem poder invocar qualquer desconhecimento como elemento impeditivo da correta formulação da proposta ou do integral cumprimento do contrato, não sendo aceitas reivindicações posteriores sob quaisquer alegações.

3.4 A participação neste Pregão importa ao Proponente a irrestrita aceitação das condições estabelecidas no presente edital e seus anexos, bem como a observância dos regulamentos, normas e técnicas aplicáveis.

3.5 O proponente arcará com todos os custos diretos e indiretos para a preparação e apresentação de sua proposta, independentemente do resultado do processo licitatório.

3.6 O Poder Legislativo Municipal de Santa Maria reserva o direito de revogar a presente licitação por razões de interesse público ou anulá-la, no todo ou em parte, por vício ou ilegalidade, sem que caiba direito indenizatório a quaisquer dos licitantes.

4 - DA REPRESENTAÇÃO E DO CREDENCIAMENTO

4.1 O Proponente deverá se apresentar para credenciamento junto ao Pregoeiro por um representante que, devidamente munido de documento que o credencie a participar deste procedimento licitatório, venha a responder por seu representado, devendo, ainda, no ato de entrega dos envelopes, identificar-se exibindo a Carteira de Identidade ou outro documento equivalente.

4.2 O credenciamento far-se-á por meio de instrumento público ou particular de procuração com firma reconhecida (**Anexo IX**), **desde que constem poderes para formular ofertas e lances de preços, bem como praticar todos os demais atos pertinentes ao certame**, em nome do proponente. Sendo sócio(a), proprietário(a), dirigente ou assemelhado da empresa proponente, seus poderes para exercer direitos e assumir obrigações em nome da empresa, deverão estar expressamente dispostos no Estatuto ou Contrato Social.

4.3 A não apresentação de documento que credencie o(a) representante, não desclassificará ou inabilitará o Licitante, mas impedirá que o(a) representante se manifeste e responda em seu nome.

4.4 É facultado ao Licitante o direito de não estar presente na sessão pública de Licitação, devendo, para tanto, enviar, se for o caso, a **declaração de enquadramento como Microempreendedor Individual, Microempresa ou Empresa de Pequeno Porte (Anexo III)**, conforme item 4.9, em envelope separado da Proposta de Preços e dos Documentos de Habilitação.

4.5 Apresentar cópia de Documento de Identidade do representante, sócio(a), proprietário(a), diretor(a) da empresa ou equivalente que venha participar do certame.

4.6 Apresentar cópia do Estatuto, Contrato Social ou documento equivalente, em vigor, devendo estarem acompanhados de todas as alterações efetuadas ou da consolidação respectiva.

4.7 Apresentar declaração dando ciência de que cumpre plenamente os requisitos habilitatórios (**Anexo VIII**). A ausência deste documento impede a empresa de participar do certame.

4.8 Para os Licitantes com representantes na sessão pública, os documentos solicitados nos itens 4.5, 4.6 e 4.7 deverão constar **FORA** do envelope da documentação e ser entregues ao Pregoeiro, que fará o credenciamento dos participantes.



4.9 Os Microempreendedores Individuais, as Microempresas e Empresas de Pequeno Porte, para assegurarem o estabelecido na Lei Complementar Federal nº 123/2006 e na Lei Municipal nº 5.245/2009, que instituem, respectivamente, o Estatuto Nacional da Microempresa e Empresa de Pequeno Porte e a Lei Geral Municipal da Microempresa, Empresa de Pequeno Porte e Microempreendedor Individual, deverão apresentar para o Pregoeiro, no ato da abertura do procedimento licitatório (credenciamento), **declaração de enquadramento como Microempreendedor Individual, Microempresa ou Empresa de Pequeno Porte (Anexo III)**, devidamente assinada pelo responsável pela sua contabilidade ou **documento fornecido pela Junta Comercial (com validade de 90 dias)**.

4.10 Caso algum dos documentos solicitados esteja dentro do envelope da documentação ou da proposta, o Pregoeiro poderá solicitar que o representante abra o envelope e retire o documento, lacrando-o logo em seguida.

4.11 Somente será efetivado o credenciamento dos Licitantes que não estejam listados no Cadastro Nacional de Empresas Inidôneas e Suspensas (**CEIS**) e no Cadastro Nacional de Empresas Punidas (**CNEP**).

4.12 A partir do término do credenciamento dos Licitantes por parte do Pregoeiro, não mais serão admitidos novos proponentes, dando-se início à sessão do certame.

5 - DA APRESENTAÇÃO DOS ENVELOPES

5.1 A Proposta de Preços e a Documentação que a instruir, deverão ser apresentadas, impreterivelmente, até o dia, hora e local já fixados no início deste Edital, em 02 (dois) envelopes (da proposta e da habilitação), devidamente fechados e rubricados no fecho.

5.2 Não será aceita, em qualquer hipótese, a participação do Licitante retardatário, a não ser na qualidade de ouvinte.

5.3 Os documentos emitidos através da internet não necessitam de autenticação, ficando sujeitos à verificação por parte do Pregoeiro.

5.4 Poderão ser feitas autenticações de documentos, diretamente no órgão licitante, pela Comissão Permanente de Licitações, preferencialmente até o último dia útil que anteceder a abertura dos envelopes.

5.5 Os Licitantes que deixarem de apresentar quaisquer dos documentos exigidos no envelope de Documentação, ou os que os apresentarem irregulares, em desacordo ao estabelecido neste Edital, serão inabilitados, não se admitindo complementação posterior.

5.6 A abertura dos envelopes da **Proposta e da Documentação** será realizada em sessão pública, da qual se lavrará ata circunstanciada, assinada pelo Pregoeiro, consignando, se for o caso, os registros efetuados pelos representantes legais dos Licitantes presentes.

5.6.1 Consideradas as ressalvas contidas neste Edital, qualquer manifestação deverá ser motivada e feita no ato da sessão pelos representantes legais dos Licitantes presentes.

5.6.2 A desclassificação da proposta do Licitante importa preclusão do seu direito de participar das fases subsequentes.

5.7 Todas as propostas e os documentos da proposta vencedora serão rubricados pelo Pregoeiro e pelos representantes legais dos Licitantes presentes na sessão que assim o desejarem, devendo, para tal, dirigirem-se à mesa do Pregoeiro.



5.8 Após o credenciamento não caberá desistência das propostas, salvo por motivo justo decorrente de fato superveniente e aceito pelo Pregoeiro.

5.9 É facultado ao Pregoeiro, em qualquer fase deste Pregão, a promoção de diligência destinada a esclarecer ou completar a instrução do processo, vedada a inclusão posterior de documento ou informação que deveria constar originariamente nos envelopes das propostas ou da documentação.

5.10 O Pregoeiro poderá desconsiderar excessos de formalismos que não comprometam o interesse da Administração, a finalidade e a segurança da contratação.

5.11 Primeiramente serão abertos os envelopes contendo as PROPOSTAS DE PREÇOS, que serão lidas para todos os presentes, sendo feita a sua conferência e posterior rubrica por parte do Pregoeiro e equipe de apoio. Os interessados que desejarem conferir as propostas dos demais licitantes deverão dirigir-se à mesa do Pregoeiro.

5.12 Os envelopes deverão conter, ainda, em sua parte externa frontal, as seguintes informações:

**PREGÃO PRESENCIAL Nº 07/2019
CÂMARA MUNICIPAL DE SANTA MARIA
COMISSÃO PERMANENTE DE LICITAÇÕES
PROPOSTA DE PREÇOS - ENVELOPE Nº 01
RAZÃO SOCIAL DA EMPRESA
FONE/FAX/E-MAIL**

**PREGÃO PRESENCIAL Nº 07/2019
CÂMARA MUNICIPAL DE SANTA MARIA
COMISSÃO PERMANENTE DE LICITAÇÕES
DOCUMENTAÇÃO DE HABILITAÇÃO - ENVELOPE Nº 02
RAZÃO SOCIAL DA EMPRESA
FONE/FAX/E-MAIL**

6 - DA PROPOSTA

6.1 A **Proposta** contida no **Envelope nº 01** deverá ser apresentada na seguinte forma:

6.1.1 Em original, constar 01 (uma) via impressa em papel, em língua portuguesa, salvo quanto às expressões técnicas de uso corrente, apresentada digitalizada ou datilografada, redigida com clareza, sem emendas, rasuras, acréscimos ou entrelinhas; devidamente datada e assinada pelo representante legal em sua última folha e rubricada nas demais.

6.1.2 Fazer menção ao número deste Pregão e conter a razão social do Licitante, nome do signatário, o CNPJ, número(s) de telefone(s), de fax e e-mail, se houver, e o respectivo endereço com CEP.

6.1.3 O licitante deverá cotar o valor em reais, com até duas casas decimais (R\$ 0,00), expresso em algarismos e, de preferência, por extenso, prevalecendo este último em caso de divergência. O preço proposto deverá contemplar todas as despesas necessárias à execução do contrato, custos administrativos, comissões, lucro, leis sociais, tributos, impostos, taxas, emolumentos, serviços de terceiros, obrigações trabalhistas, previdenciárias, transporte, seguros, licenças, enfim, tudo que se fizer necessário à perfeita execução do objeto licitado, mesmo que não especificado neste edital, bem ainda, deduzidos quaisquer descontos que venham a ser concedidos.

6.1.4 A omissão da resposta de qualquer dos quesitos de avaliação, tais como, informações técnicas ou outra documentação que comprove a veracidade da informação, poderá implicar sumária desclassificação da proposta.



6.1.5 Deverá constar na proposta o nome do representante da empresa que firmará contrato com a Administração, bem como o nº do RG, CPF, endereço do representante legal e cargo ocupado.

6.2 A simples apresentação da proposta, por si só, implicará plena aceitação, por parte do licitante, de todas as condições deste edital, independentemente de transcrição.

6.3 Poderão ser apresentadas quaisquer outras informações afins que julgar necessárias ou convenientes.

6.4 Apresentar a marca cotada, que deverá ser a mesma entregue, caso a proposta venha a ser a vencedora, sob pena de recusa do recebimento do item, nos termos do Art. 55, XI, da Lei Federal nº 8.666/93.

7 - DO JULGAMENTO DAS PROPOSTAS

7.1 As Propostas serão julgadas e adjudicadas **GLOBALMENTE**, conforme definido neste Edital e seus anexos.

7.2 Conforme incisos VI e VII, do art. 11, do Decreto Municipal nº 072/2015, de 03 de agosto de 2015, o pregoeiro procederá à abertura dos envelopes contendo as propostas de preços e classificará o autor da proposta de menor preço e aqueles que tenham apresentado propostas em valores sucessivos e superiores em até 10% (dez por cento), relativamente à de menor preço.

7.2.1 Quando não forem verificadas, no mínimo, três propostas escritas de preços nas condições definidas acima, o pregoeiro classificará os autores das melhores propostas, até o máximo de três, para que ofereçam novos lances verbais e sucessivos, quaisquer que sejam os preços oferecidos nas propostas escritas.

7.2.2 Havendo empate na classificação da terceira melhor proposta, todos os licitantes dessas propostas serão convocados a oferecer lances verbais.

7.2.3 Aos proponentes proclamados conforme o item acima será oportunizado nova disputa, por meio de lances verbais e sucessivos, de valores distintos e decrescentes, começando pelo proponente que ofertou o maior valor e os demais em ordem decrescente de valor.

7.3 Não poderá haver desistência dos lances ofertados, sujeitando-se o proponente desistente às sanções administrativas constantes neste Edital.

7.4 Após esse ato, será encerrada a etapa competitiva e ordenadas as ofertas, exclusivamente pelo critério do MENOR PREÇO GLOBAL.

7.5 Sendo aceitável a oferta, será verificado o atendimento das condições habilitatórias do Licitante que a tiver formulado.

7.6 Se a oferta não for aceitável ou se o Licitante não atender às exigências editalícias, o Pregoeiro examinará as ofertas subsequentes, na ordem de classificação, até a apuração de uma proposta que atenda a todas as exigências, sendo o respectivo Licitante declarado vencedor e o processo encaminhado à autoridade superior para homologação e adjudicação do objeto definido neste Edital e seus anexos.

7.7 Para efeitos da Lei Complementar Federal nº 123 consideram-se Microempresas ou Empresas de Pequeno Porte a Sociedade Empresária, a Sociedade Simples e o Empresário a que se refere o art. 966 da Lei Federal nº. 10.406, de 10 de janeiro de 2002, devidamente registrados no Registro de Empresas Mercantis ou no Registro Civil de Pessoas Jurídicas, conforme legislação vigente.



7.8 Da reunião lavrar-se-á ata circunstanciada, na qual serão registradas as ocorrências relevantes e que, ao final, deverá obrigatoriamente ser assinada pelo Pregoeiro e Licitantes presentes, ressaltando-se que poderá constar a assinatura da equipe de apoio, sendo-lhes facultado este direito.

7.9 Não serão consideradas as propostas que deixarem de atender, no todo ou em parte, qualquer das exigências deste Edital, observadas as demais disposições deste instrumento.

7.10 Os preços finais propostos serão considerados completos e suficientes para a execução do Contrato, objeto desta Licitação, sendo desconsiderada qualquer reivindicação de pagamento adicional quando devida a erro ou má interpretação de parte do Licitante.

7.11 Finalizadas as etapas de lance e negociação, o Licitante vencedor habilitado no certame será chamado pelo Pregoeiro, a fim de pormenorizar os valores individuais de sua proposta final.

8 - DA VALIDADE DAS PROPOSTAS

8.1 A Proposta deverá ter validade mínima de **60 (sessenta) dias** contados da data prevista no início deste Edital para o recebimento e abertura dos envelopes Documentação e Proposta.

8.2 Se, por motivo de força maior, a adjudicação não puder ocorrer dentro do período de validade da proposta, ou seja, 60 (sessenta) dias, e caso persista o interesse da Câmara Municipal de Vereadores de Santa Maria, esta poderá solicitar prorrogação geral da validade referida a todos os Licitantes classificadas, por igual prazo, no mínimo.

8.3 Decorridos 60 (sessenta) dias da data do recebimento e início da abertura dos envelopes, sem solicitação ou convocação de que tratam os itens 8.1 e 8.2 deste Edital, respectivamente, os Licitantes ficam liberados dos compromissos assumidos.

9 - DA HABILITAÇÃO

9.1 Somente poderão participar desta licitação empresas brasileiras ou empresas estrangeiras em funcionamento no Brasil, que atuam no ramo do objeto licitado.

9.4.1 Qualquer documento apresentado na fase do credenciamento será considerado como já apresentado, para fins de habilitação.

9.2 Para fins de **Habilitação Jurídica** deverá ser apresentado, conforme o caso:

9.2.1 Registro comercial, no caso de empresa individual; ou

9.2.2 Ato constitutivo, estatuto ou contrato social em vigor, devidamente registrados, em se tratando de sociedades empresariais, e, no caso de sociedades por ações, acompanhados de documentos de eleição de seus administradores; ou

9.2.3 Inscrição do ato constitutivo, no caso de sociedades simples, com indicação dos sócios responsáveis pela administração; ou

9.2.4 Decreto de autorização, quando se tratar de empresa ou sociedade estrangeira em funcionamento no País, e ato de registro ou autorização para funcionamento expedido pelo órgão competente, em vigência, quando a atividade assim o exigir.



9.2.5 Os documentos acima deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

9.2.6 O licitante deve declarar, sob as penalidades cabíveis, **que não foi declarado inidôneo e que inexistente fato que possa impedir sua habilitação neste certame**, inclusive na vigência contratual, caso venha a ser contratado pela Câmara Municipal de Santa Maria, conforme modelo de declaração (**Anexo VI**).

9.2.7 O licitante deve declarar, sob as penalidades cabíveis, o cumprimento do disposto no **art. 27, V da Lei nº 8.666/93**, conforme modelo de declaração (**Anexo VII**).

9.2.8 Apresentar **Certidão negativa de falência, recuperação judicial ou recuperação**, expedida pelo distribuidor do foro da comarca da sede da pessoa jurídica, ou, no caso de empresa individual, certidão negativa de execução patrimonial expedida no domicílio da pessoa física, que terá a validade de 90 (noventa) dias após sua emissão.

9.3 Para verificação da **Regularidade Fiscal e Trabalhista** deverá ser apresentado:

9.3.1 Prova de inscrição no Cadastro Nacional da Pessoa Jurídica – CNPJ.

9.3.2 Prova de inscrição no Cadastro de Contribuintes do Município através de alvará (de localização ou de funcionamento) relativo ao domicílio ou sede do cadastro, pertinente ao seu ramo de atividade e compatível com o objeto contratual.

9.3.3 Prova de regularidade para com os **Tributos Federais** - certidão negativa de débito ou positiva com efeitos de negativa, relativamente a débitos de tributos e contribuições federais e dívida ativa da União.

9.3.4 Prova de regularidade para com a **Fazenda Estadual** – certidão negativa de débito ou positiva com efeitos de negativa – do domicílio ou sede da empresa ou outra equivalente na forma da lei.

9.3.5 Prova de regularidade para com a **Fazenda Municipal** – certidão negativa de débito ou positiva com efeitos de negativa – do domicílio ou sede da empresa ou outra equivalente na forma da lei.

9.3.6 Certificado de regularidade para com o **FGTS**.

9.3.7 Prova de regularidade para com a Justiça do Trabalho, por meio da **Certidão Negativa de Débitos Trabalhistas – CNDT**, emitida pelo Tribunal Superior do Trabalho, nos termos da lei nº 12.440/2011.

9.4 Para verificação da **qualificação técnica**:

9.4.1 Apresentar, no mínimo, 01 (um) atestado de capacidade técnica, emitidos por órgão da administração pública ou por empresa privada, para os quais a proponente tenha fornecido mão de obra terceirizada semelhantes ao objeto desta licitação, devendo estar expressos nos atestados todas as características dos serviços prestados, como:

9.4.1.1. identificação da pessoa jurídica eminente;

9.4.1.2. nome e cargo do signatário;

9.4.1.3. endereço completo do eminente;

9.4.1.4. período de vigência do contrato;

9.4.1.5. objeto contratual;

9.4.1.6. quantitativos executados;



9.4.1.7. outras informações técnicas necessárias e suficientes para a avaliação das experiências referenciadas pela Comissão de Licitação.

9.5 - Observações:

9.5.1 Todos os documentos de habilitação emitidos em língua estrangeira deverão ser entregues acompanhados da tradução para língua portuguesa, efetuada por Tradutor Juramentado, e também devidamente consularizados ou registrados no Cartório de Títulos e Documentos. Bem como, documentos de procedência estrangeira, emitidos em língua portuguesa, também deverão ser apresentados devidamente consularizados ou registrados no Cartório de Títulos e Documentos.

9.5.2 Os documentos solicitados neste edital, deverão ser emitidos em papéis timbrados dos Órgãos ou das Empresas que os expedirem.

9.5.3 O representante legal que assinar documentos pela empresa, deverá estar investido de poderes para esse fim e comprovar tal competência caso a Comissão de Licitação vier a exigir.

9.5.4 Os documentos pertinentes e exigidos neste Edital, dentro do Envelope nº 02, deverão, de preferência, ser entregues numerados sequencialmente e na ordem indicada, a fim de permitir maior rapidez durante a conferência e exame correspondente.

9.5.5 Sob pena de inabilitação, todos os documentos apresentados para habilitação deverão estar:

9.5.5.1 em nome do Licitante e, preferencialmente, com número do CNPJ e endereço respectivo;

9.5.5.2 em nome da matriz, se o Licitante for a matriz;

9.5.5.3 em nome da filial, se o Licitante for a filial;

9.5.5.3.1 serão dispensados da filial aqueles documentos que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz;

9.5.5.4 datados dos últimos **180 (cento e oitenta) dias** até a data de abertura do **Envelope nº 01**, quando não tiver prazo estabelecido pelo órgão/empresa competente expedidor(a);

9.5.5.4.1 não se enquadram no prazo de que trata este item os documentos que, pela própria natureza, não apresentam prazo de validade.

9.5.6 Os documentos exigidos neste Pregão poderão ser apresentados em original, por qualquer processo de cópia autenticada por Cartório competente ou por membro da Comissão de Licitação ou publicação em órgão da imprensa oficial.

9.5.7 Serão aceitas somente cópias legíveis.

9.5.8 Não serão aceitos documentos cujas datas estejam rasuradas.

9.5.9 O Pregoeiro reserva-se o direito de solicitar o original de qualquer documento, sempre que julgar necessário.

9.5.10 Se a documentação da habilitação não estiver completa e correta ou contrariar qualquer dispositivo deste Edital e seus anexos, o Pregoeiro considerará o proponente inabilitado, observados os Princípios da Proporcionalidade e Razoabilidade, Contraditório e Ampla Defesa.

9.5.11 O licitante poderá apresentar Certificado de Registro Cadastral - CRC atualizado emitido por qualquer órgão da Administração Pública, em substituição a certidões arroladas no item 9.2 deste edital, desde que mencione as datas de validade das certidões.

9.5.12 O Microempreendedor Individual, a Microempresa e a Empresa de Pequeno Porte que possuir



restrição em qualquer dos documentos de regularidade fiscal e trabalhista, previstos neste Edital, terá sua habilitação condicionada à apresentação de nova documentação que comprove a sua regularidade, **em até 05 (cinco) dias úteis**, a contar da data em que for declarada como vencedora do certame.

9.5.12.1 O benefício de que trata o item anterior não eximirá o Microempreendedor Individual, a Microempresa e a Empresa de Pequeno Porte da apresentação de todos os documentos exigidos neste Edital, ainda que apresentem alguma restrição.

9.5.12.2 O prazo descrito no item acima poderá ser prorrogado, uma única vez, por igual período, a critério da Administração, desde que seja requerido pelo interessado, devidamente justificado e durante o transcurso do prazo original.

9.5.12.3 A não regularização da documentação nos termos acima descritos implicará decadência do direito à contratação, sendo facultado à Administração, uma vez observado o disposto no item **9.5.12.5**, convocar os Licitantes remanescentes, na estrita ordem de classificação, para a assinatura do Contrato, ou revogar a Licitação.

9.5.12.4 Não terá direito ao benefício de que trata este item o Microempreendedor Individual, a Microempresa e a Empresa de Pequeno Porte que tenha deixado de apresentar ou apresente irregular algum dos documentos relativos à Regularidade Jurídica.

9.5.12.5 Ocorrendo a situação descrita no item **9.5.12**, será verificada, também, a documentação de habilitação dos demais Licitantes que apresentarem propostas ao mesmo item, na exata ordem das propostas classificadas, até que seja encontrado, pelo menos, 01 (um) com habilitação regular, de forma a garantir o andamento do certame no caso de o Licitante beneficiário não demonstrar sua regularidade no prazo legalmente previsto para tanto, de acordo com o que dispõem o art. 43, §§ 1º e 2º da Lei Complementar Federal nº 123/2006 e art. 30, §§ 1º, 2º e 3º da Lei Municipal nº 5.245/2009.

10 - DA IMPUGNAÇÃO DO ATO CONVOCATÓRIO

10.1 Em **até 02 (dois) dias úteis** antes da data fixada para recebimento das propostas, qualquer pessoa poderá solicitar esclarecimentos, providências ou impugnar o ato convocatório do Pregão.

10.2 Não serão reconhecidas as impugnações depois de vencidos os respectivos prazos legais.

10.3 Em regra, a impugnação deverá ser entregue no Setor de Protocolo da Câmara Municipal de Vereadores, por via postal ou pessoalmente, devendo respeitar, obrigatoriamente, o prazo definido no item 10.1 deste Edital.

10.4 Quando as impugnações forem enviadas via e-mail, os originais deverão ser entregues no Setor de Protocolo da Câmara de Vereadores deste Município, necessariamente, **até 05 (cinco) dias contínuos** da data do término do prazo estabelecido no item 10.1 deste Edital.

10.4.1 O licitante ou pessoa que se utilizar dessa forma de transmissão, torna-se responsável pela qualidade e fidelidade do material transmitido, bem como por sua entrega neste Órgão.

10.5 Caberá ao Pregoeiro decidir sobre a petição no prazo de **24 (vinte e quatro) horas**.

11 - DO DIREITO DE PETIÇÃO E DOS RECURSOS

11.1 Declarado o vencedor, qualquer Licitante poderá manifestar imediata e motivadamente a intenção de recorrer, quando lhe será concedido o prazo de **03 (três) dias** para a apresentação das razões de recurso, ficando os demais Licitantes desde logo intimados para apresentar as contrarrazões, em igual número de dias, que começarão a correr do término do prazo do recorrente, sendo-lhes assegurada vista imediata dos autos.



11.2 A falta de manifestação imediata e motivada do Licitante importará a decadência do direito de recurso.

11.3 Qualquer recurso e impugnação contra a decisão do Pregoeiro, **não terá efeito suspensivo**.

11.4 O acolhimento do recurso importará a invalidação apenas dos atos insuscetíveis de aproveitamento.

11.5 A petição poderá ser feita na própria sessão de recebimento, e, se oral, será reduzida a termo em ata.

11.6 Os autos do processo permanecerão com vista franqueada aos interessados na Câmara Municipal de Vereadores de Santa Maria, situada na Rua Vale Machado, n.º 1415, Centro, Santa Maria, RS, junto a Comissão de Licitações, nos dias úteis no horário de expediente externo.

12 - DA ADJUDICAÇÃO

12.1 O objeto deste Pregão será adjudicado **GLOBALMENTE**, depois de atendidas as condições estabelecidas neste Edital.

13 - DO TERMO DE CONTRATO

13.1 Contratação de empresa capacitada para prestar serviço de solução para gerenciamento de conectividade de redes e prevenção de ameaças com suporte remoto para até 180 usuários, conforme Termo de Referência (**Anexo II**), será formalizado e conterà, necessariamente, as condições já especificadas neste ato convocatório e seus anexos.

13.2 A Administração da Câmara convocará o Licitante vencedor, durante a validade da sua proposta, para, no prazo máximo de até **05 (cinco) dias úteis**, assinar o contrato, aceitar ou retirar o instrumento equivalente sob pena de decair o direito à contratação, sem prejuízo das sanções previstas no art. 81 da Lei nº 8.666/93.

13.3 O prazo da convocação poderá ser prorrogado uma vez, por igual período, quando solicitado pelo Licitante vencedor durante o seu transcurso, desde que ocorra motivo justificado e aceito pela Administração da Câmara.

13.4 Será informado o nome do representante da empresa que firmará contrato com a Administração, bem como o nº do RG, CPF e cargo ocupado.

13.5 É facultado à Administração da Câmara, quando o convocado não assinar o referido documento no prazo e nas condições estabelecidos, chamar os licitantes remanescentes, obedecida a ordem de classificação, para fazê-lo em igual prazo e nas mesmas condições propostas pelo primeiro classificado, inclusive quanto aos preços atualizados, ou revogar este Pregão, independentemente da cominação prevista no art. 81 da Lei nº 8.666/93.

13.6 A recusa injustificada do licitante vencedor em assinar o Contrato, aceitar ou retirar o instrumento equivalente, dentro do prazo estabelecido pela Administração da Câmara, caracteriza o descumprimento total da obrigação assumida, sujeitando-o às penalidades legalmente estabelecidas.

13.6.1 O disposto no subitem anterior não se aplica aos licitantes convocados nos termos do § 2º do art. 64 da Lei nº 8.666/93 que não aceitarem a contratação nas mesmas condições propostas pelo adjudicatário, inclusive quanto ao prazo e preço.



14 – DAS SANÇÕES ADMINISTRATIVAS

14.1 Comete infração administrativa, nos termos da Lei Federal nº 10.520, de 2002, o licitante/adjudicatário que:

14.1.1 não assinar o contrato quando convocado dentro do prazo de validade da proposta ou não assinar o termo de contrato decorrente deste Pregão;

14.1.2 apresentar documentação falsa;

14.1.3 deixar de entregar os documentos exigidos no certame;

14.1.4 ensejar o retardamento da execução do objeto;

14.1.5 não manter a proposta;

14.1.6 cometer fraude fiscal;

14.1.7 comportar-se de modo inidôneo.

14.2 Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como Microempreendedor Individual, Microempresa ou Empresa de Pequeno Porte ou o conluio entre os licitantes, em qualquer momento da Licitação, mesmo após o encerramento da fase de lances.

14.3 O licitante/adjudicatário que cometer qualquer das infrações discriminadas no subitem anterior ficará sujeito, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

14.3.1 Multa de 1% (um por cento) sobre o valor estimado do(s) item(s) prejudicado(s) pela conduta do licitante;

14.3.2 Impedimento de licitar com a Administração Pública, pelo prazo de até 05 (cinco) anos;

14.4 A penalidade de multa pode ser aplicada cumulativamente com a sanção de impedimento.

14.5 A aplicação de qualquer das penalidades previstas realizar-se-á mediante prévio e regular processo administrativo, que assegurará, absolutamente, o contraditório e a ampla defesa ao licitante/adjudicatário, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente na Lei nº 9.784, de 1999.

14.6 A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o Princípio da Proporcionalidade e Razoabilidade.

15 - DA FORMA, DO PRAZO E DO LOCAL DE ENTREGA DOS OBJETOS

15.1 A implantação dos itens contratados deverá ser feita em absoluta conformidade com o previsto e nos prazos estabelecidos neste Edital, contados da data de assinatura do Contrato.

15.2 Os itens contratados deverão ser implantados no ambiente computacional da CONTRATANTE localizada na Rua Vale Machado, 1415, CEP 97010.530 – Santa Maria/RS, em dias úteis e em horário de expediente.

15.3 O prazo para implantação dos itens será de 20 (vinte) dias, a contar da data de assinatura do contrato, podendo ser prorrogado por igual período, desde que apresente justificativa por escrito e previamente autorizada pela autoridade competente para celebrar o contrato.

15.4 Corre por conta do vencedor qualquer prejuízo causado ao patrimônio da Câmara Municipal de Vereadores de Santa Maria por conta de ação de seus empregados quando da execução ou entrega dos serviços contratados.



16 - DOS RECURSOS ORÇAMENTÁRIOS

16.1 Os recursos orçamentários desta contratação correrão por conta das seguintes dotações orçamentárias:

011220001.2.108 – Manutenção das Atividades Administrativas;
3.3.90.40.06 – Locação de Softwares.

17 - DO PAGAMENTO

17.1 O pagamento será efetuado **em até 05 (cinco) dias úteis** após liquidação da Nota Fiscal, que deverá estar devidamente visada pelo responsável pelo recebimento e conferência do objeto contratado. O pagamento será conforme as etapas já concluídas.

17.2 Não haverá, sob qualquer hipótese, qualquer pagamento adiantado à efetiva entrega do objeto contratado.

17.3 Os pagamentos far-se-ão em moeda corrente nacional e serão creditados em nome do Contratado, **após o efetivo cumprimento do objeto contratado devidamente atestado pela fiscalização**, mediante ordem bancária em conta corrente indicada pela Empresa ou por meio de ordem bancária para o pagamento de Nota(s) Fiscal(is), Fatura(s) ou Documento de Cobrança de Valor Jurídico Equivalente, com “código de barras”, uma vez satisfeitas as condições estabelecidas neste Edital.

17.3.1 Serão descontadas do valor do pagamento as eventuais multas que lhe tenham sido impostas em decorrência de inadimplência contratual.

17.3.2 Qualquer erro ou omissão havido na documentação fiscal ou na fatura será objeto de correção pela empresa e haverá, em decorrência, suspensão do prazo de pagamento até que o problema seja definitivamente regularizado.

17.3.3 A Câmara de Vereadores reserva-se o direito de suspender o pagamento se o objeto for prestado em desacordo com as especificações constantes deste instrumento.

17.4 Tendo sido impostas penalidades ao CONTRATADO das quais não tenha recorrido tempestivamente, ou que já tenham sido objeto de decisão administrativa transitada em julgado, o respectivo valor será descontado do pagamento devido.

17.5 Todo e qualquer pagamento poderá ser sustado, se verificada qualquer das hipóteses a seguir elencadas e enquanto perdurar o ato/fato/omissão que a tiver motivado, sem direito a posterior reajuste, acréscimo, lucros cessantes, indenização, juros e/ou correção monetária:

17.5.1 retardar injustificadamente a execução do objeto da presente licitação;

17.5.2 haver infração à condição ou obrigação estabelecida no edital, contrato ou na proposta apresentada.

17.6 Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido, de alguma forma, para tanto, fica convencionado que a taxa de compensação financeira devida pela Contratante, entre a data do vencimento e o efetivo adimplemento da parcela, é calculada mediante a aplicação da seguinte fórmula:

$$EM = I \times N \times VP$$

17.6.1 Sendo:

EM = Encargos moratórios;

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;



VP = Valor da parcela a ser paga.

I = Índice de Compensação Financeira = 0,00016438

17.6.1.1 O Índice de Compensação Financeira (I) mencionado no subitem anterior é apurado da seguinte forma

$I = (TX = \text{Percentual da Taxa Anual} = 6\%)$

$I = (6 / 100) / 365$

$I = 0,00016438$

18 - DO REAJUSTE E DO REEQUILÍBRIO ECONÔMICO-FINANCEIRO

18.1 O preço do Contrato poderá ter seu valor mensal reajustado, após o primeiro ano de vigência, utilizando-se o índice acumulado dos últimos 12 (doze) meses do IGP-M – ÍNDICE GERAL DE PREÇOS DO MERCADO (Instituto Brasileiro de Geografia e Estatística).

18.2 Os preços do Contrato poderão ser recompostos, em consonância com o que dispõe o artigo 65, inciso II, alínea “d”, da Lei Federal 8.666/1993.

19 DO FORO

19.1 As questões decorrentes da execução do objeto deste Edital que não possam ser dirimidas administrativamente, serão processadas e julgadas no **Foro da Comarca de Santa Maria – RS**, com exclusão de qualquer outro, por mais privilegiado que seja.

20 - DAS DISPOSIÇÕES GERAIS

20.1 É facultado 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 documentos ou informações que deveriam constar no ato da sessão pública.

20.2 As Empresas Estrangeiras ficam obrigadas a apresentar todos os documentos do presente procedimento licitatório em Língua Portuguesa.

20.3 Fica assegurado à Câmara Municipal de Vereadores de Santa Maria o direito de, no interesse da Administração, anular ou revogar, a qualquer tempo, no todo ou em parte, a presente Licitação, dando ciência aos participantes, na forma da legislação vigente.

20.4 Os proponentes assumem todos os custos de preparação e apresentação de suas propostas, que, em nenhum caso, serão repassados à Câmara de Vereadores, independentemente da condução ou do resultado do processo licitatório.

20.5 Os proponentes são responsáveis pela fidelidade e legitimidade das informações e dos documentos apresentados em qualquer fase da Licitação.

20.6 Após apresentação da proposta, não caberá desistência, salvo por motivo justo decorrente de fato superveniente e aceita pelo Pregoeiro.

20.7 Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a realização de certame na data marcada, a sessão será automaticamente transferida para o **primeiro dia útil subsequente**, no mesmo horário e local, anteriormente estabelecidos, desde que não haja comunicação do Pregoeiro em contrário.



20.8 Os prazos estabelecidos neste Edital e seus anexos só se iniciam e vencem em dias de expediente, caso em que, na sua contagem, excluir-se-á o dia do início e incluir-se-á o do vencimento.

20.9 O desatendimento de exigências formais não essenciais não importará no afastamento do Licitante, desde que sejam possíveis as aferições das suas qualificações e as exatas compreensões da sua proposta, durante a realização da sessão pública de pregão.

20.10 As normas que disciplinam este Pregão serão sempre interpretadas em favor da ampliação da disputa entre os interessados, sem comprometimento da segurança do futuro Contrato.

20.11 Aos casos omissos aplicar-se-ão as demais disposições pertinentes constantes nos diplomas normativos previstos no preâmbulo deste Edital.

20.12 Qualquer pedido de esclarecimento em relação a eventuais dúvidas na interpretação do presente Edital e seus anexos deverá ser encaminhado, por escrito, ao Pregoeiro, na Câmara Municipal de Vereadores de Santa Maria, situada à Rua Vale Machado, 1415, Comissão Permanente de Licitações ou por meio do e-mail licitacoes@camara-sm.rs.gov.br.

20.12.1 As dúvidas a serem dirimidas por telefone serão somente aquelas de ordem estritamente informal.

21 - DOS ANEXOS

21.1 São partes integrantes deste Edital os seguintes anexos:

ANEXO I - Minuta de Contrato;

ANEXO II - Termo de Referência;

ANEXO III - Modelo de Declaração de Enquadramento como Microempreendedor Individual, Microempresa ou Empresa de Pequeno Porte;

ANEXO IV - Do Valor Máximo Unitário e Total Admitidos por Item;

ANEXO V - Modelo de Proposta de Preço;

ANEXO VI - Modelo de Declaração de que o proponente não foi declarado inidôneo e que inexistente fato impeditivo para licitar e contratar com a Administração Pública;

ANEXO VII - Modelo de Declaração para atendimento ao disposto no art. 27, V, da Lei nº 8.666/93;

ANEXO VIII - Modelo de Declaração de cumprimento dos requisitos de habilitação;

ANEXO IX - Modelo de Procuração;

ANEXO X - Portaria nº 73/2019 – Designação do Pregoeiro e da Equipe de Apoio.

Santa Maria, 12 de junho de 2019.

Ver(a). MARIA APARECIDA BRIZOLA MAYER
Presidente da CMVSM



ANEXO I - MINUTA DO CONTRATO

CONTRATO Nº NRCONTR

Contrato para contratação de empresa capacitada para prestar serviço de solução para gerenciamento de conectividade de redes e prevenção de ameaças com suporte remoto para até 180 usuários, que celebram entre si a Câmara Municipal de Vereadores de Santa Maria e a empresa _____, conforme Processo Licitatório nº 51/2019, Pregão Presencial nº 07/2019.

PREÂMBULO

A **CÂMARA MUNICIPAL DE VEREADORES DE SANTA MARIA (CMVSM)**, inscrita no CNPJ sob o número 89.250.708/0001-04, situada na Rua Vale Machado, nº 1415, nesta cidade, representada neste ato pela sua Presidente, Sra. Vereadora MARIA APARECIDA BRIZOLA MAYER, doravante denominada **CONTRATANTE**, e de outro lado a _____, inscrita no CNPJ/MF sob o nº _____, Inscrição Estadual nº _____, Inscrição Municipal nº _____, localizada na rua _____, na cidade de _____, CEP _____, telefone _____, doravante denominada **CONTRATADA**, neste ato representada pelo(a) Sr(a). _____, portador(a) da Cédula de Identidade nº _____, CPF nº _____, residente à _____, resolvem celebrar o presente Contrato, que será regido pela Lei Federal nº 10.520, de 17 de julho de 2002, pelo Decreto Municipal nº 072/2015, de 03 de agosto de 2015, que institui a modalidade Pregão no Município de Santa Maria, pela Lei Federal nº 8.666/1993, pelas demais normas federais e municipais pertinentes, no que couberem, e pelo constante do **Processo Licitatório nº 51/2019, Pregão Presencial nº 07/2019**. O Edital e a proposta da CONTRATADA, independentemente de sua transcrição, passam a fazer parte integrante e complementar deste instrumento, que se regerá pelas seguintes cláusulas e condições:

CLÁUSULA I – DO OBJETO

1.1. O presente Contrato tem por objeto a contratação de empresa capacitada para prestar serviço de solução para gerenciamento de conectividade de redes e prevenção de ameaças com suporte remoto para até 180 usuários, conforme Termo de Referência – Anexo II do Edital da Licitação;

1.1.1. Planilha de quantitativos:

| Item | Descrição | Quantidade |
|------|--|------------|
| 1 | Atualização anual das vacinas e software, caso necessário (a partir do segundo ano). | 170 |
| 2 | Solução de segurança para servidores (licença de uso para antivírus, somente no primeiro ano). | 3 |
| 3 | Aquisição de software para solução endpoint (licença de software, somente no primeiro ano). | 167 |
| 4 | Suporte técnico remoto (mensal e permanente durante a vigência do contrato – estimado em 120 horas para 12 meses). | 12 meses |
| 5 | Instalação e treinamento remoto inicial, a ser pago uma única vez, no primeiro ano somente. | 1 |
| 6 | Solução para gerenciamento de conectividade de redes (mensal e permanente durante a vigência do contrato). | 12 meses |



1.2. CARACTERÍSTICAS GERAIS DA SOLUÇÃO PARA GERENCIAMENTO DE CONECTIVIDADE DE REDES:

1.2.1. A solução deverá ser composta por 1 appliance física contendo todos os softwares necessários para o seu correto e perfeito funcionamento, monitoramento e gerenciamento;

1.2.2. A solução deve ser de um único fabricante e possuir arquitetura de hardware dedicada (não x86);

1.2.3. A solução deverá suportar, com todos os serviços internos ativos (antivírus, firewall, VPN, IPS, etc.), um link de 100Mbps dedicado e com cerca de 300 dispositivos conectados sem degradação de performance do link; além disso suportar (fazendo substituição/upgrade de equipamento se necessário), dentro de 3 anos, um possível incremento do link dedicado para 200Mbps dedicado e aumento do número de dispositivos conectados para 600 sem degradação do link também;

1.2.4. Cada appliance deve atender no mínimo aos seguintes requisitos (características de hardware e performance):

1.2.4.1. Throughput de, no mínimo, 4.4 Gbps com a funcionalidade de firewall habilitada para tráfego IPv4 e IPv6, independentemente do tamanho do pacote;

1.2.4.2. Suporte a, no mínimo, 2M conexões simultâneas;

1.2.4.3. Suporte a, no mínimo, 30.000 novas conexões por segundo;

1.2.4.4. Throughput de, no mínimo, 4 Gbps de VPN IPsec;

1.2.4.5. Estar licenciado para ou suportar sem o uso de licença, 2K túneis de VPN IPSEC Site-to-Site simultâneos;

1.2.4.6. Estar licenciado para ou suportar sem o uso de licença, 10K túneis de clientes VPN IPSEC simultâneos;

1.2.4.7. Throughput de, no mínimo, 200 Mbps de VPN SSL;

1.2.4.8. Estar licenciado para no mínimo, 5K clientes de VPN SSL simultâneos;

1.2.4.9. Suportar no mínimo 500 Mbps de throughput de IPS;

1.2.4.10. Suportar no mínimo 130 Mbps de throughput de Inspeção SSL;

1.2.4.11. Throughput de, no mínimo, 360 Mbps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS, Antivírus e Antispyware. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o menor valor será aceito;

1.2.4.12. Possuir ao menos 8 interfaces 1Gbps Ethernet RJ45;

1.2.4.13. Possuir ao menos 2 interfaces 1Gbps Ethernet SPF;

1.2.4.14. Estar licenciado e/ou ter incluído sem custo adicional, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance;

1.2.4.15. Suporte a, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance;

1.2.4.16. Possuir armazenamento interno de no mínimo 420 GB para armazenar logs;

1.2.4.17. Para fim de aferição das taxas definidas nos itens **1.2.4.1.** a **1.2.4.19**, considerar-se-ão apenas informações contidas em documentos de domínio público do fabricante;

1.2.4.18. A solução deve ter altura máxima de 2U;

1.2.4.19. A solução deve funcionar em 110-240V 50-60Hz, definido automaticamente pelo aparelho.

1.2.5. A solução deverá estar instalada e configurada no prazo de 20 dias a partir da data de assinatura do contrato.

1.3. CARACTERÍSTICAS DA SOLUÇÃO ANTIVÍRUS:

13.1. Suporte total aos sistemas operacionais baseados na plataforma Windows:

1.3.1.1. Windows 2012 Server Standard;

1.3.1.2. Suporte total a Windows 7, Windows 8, Windows 10;

5.1.3. Suporte total a plataforma 32 e 64 bits.



1.3.2. Todas as funcionalidades deste item devem ser ativadas por agente único que facilite a instalação, a configuração e o gerenciamento.

1.3.3. Rastreamento em tempo real, para arquivos durante entrada e saída (gravação e leitura), com as seguintes opções:

1.3.3.1. Negar acesso ao arquivo infectado e prosseguir;

1.3.3.2. Limpar o arquivo;

1.3.3.3. Apagar o arquivo infectado;

1.3.3.4. Mover o arquivo infectado para área de segurança (quarentena);

1.3.3.5. Rastreamento manual com interface Windows, customizável, com opção de limpeza;

1.3.3.6. Permitir diferentes configurações de varredura em tempo real baseando-se em processos de baixo ou alto risco, tornando assim o desempenho do produto mais estável;

1.3.3.7. Rastreamento em tempo real dos processos em memória, para a captura de vírus que são executados em memória sem a necessidade de escrita de arquivo;

1.3.3.8. Detecção de programas maliciosos como spyware, programas de propaganda, ferramentas como password crackers, etc.;

1.3.3.9. Programação de atualizações automáticas das definições de vírus, a partir de local predefinido da rede, ou de site da Internet, com frequência (no mínimo diária) e horários definidos pelo administrador;

1.3.3.10. Permitir atualização incremental da lista de definições de vírus;

1.3.3.11. Opção de downgrade de vacina via console de gerenciamento.

1.3.4. Programação de rastreamentos automáticos do sistema com as seguintes opções:

1.3.4.1. Escopo: Todos os drives locais, drives específicos, ou pastas específicas;

1.3.4.2. Ação: Somente alertas, limpar automaticamente, apagar automaticamente, renomear automaticamente, ou mover automaticamente para área de segurança (quarentena);

1.3.4.3. Frequência: Horária, diária, semanal, mensal;

1.3.4.4. Exclusões: Pastas ou arquivos que não devem ser rastreados;

1.3.4.5. Gerar registro (log) dos eventos de vírus em arquivo e local definido pelo administrador, com limite de tamanho opcional;

1.3.4.6. Gerar notificações de eventos de vírus através de alerta na rede;

1.3.4.7. Detectar, analisar e eliminar, automaticamente e em tempo real, programas maliciosos em:

1.3.4.8. Processos em execução em memória principal (RAM);

1.3.4.9. Arquivos criados, copiados, renomeados, movidos ou modificados, inclusive em sessões de linha de comando (DOS ou shell) abertas pelo usuário;

1.3.4.10. Arquivos compactados automaticamente, em pelo menos nos seguintes formatos: ZIP, EXE, ARJ, MIME/UU, Microsoft CAB, Microsoft Compress;

1.3.4.11. Arquivos recebidos por meio de programas de comunicação instantânea (MSN Messenger, Yahoo Messenger, Google Talk, dentre outros);

1.3.4.12. Capacidade de finalizar processos com nomes de vírus ou nomes relacionados;

1.3.4.13. Possibilidade de reparar o registro do sistema após eliminação de epidemia;

1.3.4.14. Permitir bloqueio de portas;

1.3.4.15. Permitir criação de regras baseadas em processos de sistema;

1.3.4.16. Permitir o bloqueio de compartilhamentos da máquina em caso de epidemia;

1.3.4.17. Possuir proteção contra estouro de buffer;

1.3.4.18. Capacidade de retomar atualizações do ponto onde foram interrompidas em caso de perda de conexão, sem necessidade de reinício de todo o processo;

1.3.4.19. Detecção de cookies potencialmente indesejáveis no sistema;

1.3.4.20. O sistema de antispyware deve estar totalmente integrado ao software antivírus utilizando a mesma biblioteca de definições de vírus e demais ameaças;



1.3.4.21. O sistema deve estar integrado ao console de gerenciamento de segurança de sistemas, que também gerencia antivírus, antispam e controle de acesso à rede, possibilitando uma única e simples interface para gerenciar toda uma solução de segurança. Não deve ser instalado nenhum software adicional a console de gerenciamento para permitir o controle integrado;

1.3.4.22. Oferecer proteção avançada de sistemas contra ameaças tais como ataques remotos de injeção de SQL ou HTTP;

1.3.4.23. Trabalhar no modo de quarentena permitindo a verificação pelo software de gerenciamento se o cliente está trabalhando com políticas antigas e versões desatualizadas, neste caso, o cliente é bloqueado a uma área de quarentena, limitando o acesso a rede desta estação;

1.3.4.24. Capacidade de detectar e bloquear tentativas de invasão;

1.3.4.25. Possuir instalação “silenciosa”;

1.3.4.26. Possibilidade de varredura de portas das estações de trabalho;

1.3.4.27. Possuir sistema contra vulnerabilidades de sistemas operacionais e aplicativos (principalmente Microsoft), antes de ser aplicada a correção dessas falhas nos endpoints;

1.3.4.28. Sistema de Proteção para sistemas contra vulnerabilidades não corrigidas;

1.3.4.29. Sistema de proteção contra ameaças mesmo se ainda não tiverem instalado uma correção do fornecedor que lide com uma vulnerabilidade conhecida.

1.3.5. Características do Módulo para Gerenciamento da Solução:

1.3.5.1. Programação de atualizações automáticas das listas de definições de vírus, a partir de local predefinido da rede, ou de site seguro da Internet, com frequência (no mínimo diária) e horários definidos pelo administrador da solução;

1.3.5.2. Permitir atualização incremental da lista de definições de vírus;

1.3.5.3. Atualização automática do engine do programa de proteção a partir de localização na rede local ou na Internet, a partir de fonte autenticável;

1.3.5.4. Permitir o retorno (rollback) das atualizações das listas de definições de vírus e motores de varreduras.

1.3.5.5. Gerar registro (log) dos eventos de vírus em arquivo e local definido pelo administrador da solução, com limite de tamanho opcional;

1.3.5.6. Permitir proteção das configurações da solução instalada na estação de trabalho através de senha ou controle de acesso, em ambos os casos, controlada por política gerenciada pela console de administração da solução completa;

1.3.5.7. Permitir o gerenciamento do servidor a partir de console tipo web, com acesso via https, instalada em outra máquina;

1.3.5.8. Permitir a instalação do Antivírus nos clientes a partir de um único servidor;

1.3.5.9. Permitir a criação de tarefas de atualização, verificação de vírus e upgrades em períodos de tempo pré-determinados, na inicialização do Sistema Operacional ou no Logon na rede;

1.3.5.10. Suporte a múltiplos usuários, com diferentes níveis de acesso e permissões aos produtos gerenciados;

1.3.5.11. Forçar a instalação do software Antivírus nos clientes;

1.3.5.12. Caso o cliente desinstale o software Antivírus, o mesmo deverá ser reinstalado, quando o agente verificar o ocorrido;

1.3.5.13. Customização dos relatórios gráficos gerados;

1.3.5.14. Geração de relatórios que contenham as seguintes informações:

1.3.5.14.1. Máquinas com a lista de definições de vírus desatualizada;

1.3.5.14.2. Qual a versão do software instalado em cada máquina;

1.3.5.14.3. Os vírus que mais foram detectados;

1.3.5.14.4. As máquinas que mais sofreram infecções em um determinado período de tempo;

1.3.5.14.5. Os usuários que mais sofreram infecções em um determinado período de tempo;

1.3.5.14.6. Gerenciamento de todos os módulos da suíte.

1.3.6. Característica da Solução Antivírus para Servidor:



1.3.6.1. A solução deverá permitir a sua implantação atendendo as seguintes características:

1.3.6.1.1. Multi-Plataforma, atuando para realizar o rastreamento em tempo real, por demanda e agendado de malwares, através da utilização de uma máquina com a solução Antivírus instalada efetuando todas as análises da estrutura, sem a necessidade de qualquer integração com agentes externos ou a instalação de clientes Antivírus em cada uma das máquinas;

1.3.6.2. Sistemas Operacionais Suportados para o servidor de varredura Offload:

1.3.6.2.1. Windows 2012 Server Standard;

1.3.6.3. Sistemas Operacionais Suportados nas máquinas a serem varridas em busca de ameaças:

1.3.6.3.1. Windows 7 (32 ou 64 bits);

1.3.6.3.2. Windows 8 Beta (32 ou 64 bits);

1.3.6.3.3. Windows 10 (32 ou 64 bits);

1.3.6.4. Console de Gerência da Solução:

1.3.6.4.1. Deve dar suporte à instalação em um servidor nas plataformas Windows 2012 Server Standard;

1.3.6.4.2. O Gerenciador deve trabalhar em modo Cluster;

1.3.6.4.3. O gerenciador deve prover ferramentas de Backup e Restore;

1.3.6.4.4. A ferramenta de gerência deve possibilitar autenticação externa integrada a estrutura LDAP;

1.3.6.4.5. A ferramenta de gerência deve suportar o gerenciamento de políticas de senha de autenticação na console;

1.3.6.4.6. A solução de gerenciamento deve permitir acesso a sua console via web;

1.3.6.4.7. Implementação de Dashboard com medição do nível de atualização do ambiente e o nível de cumprimento de política de segurança previamente definida;

1.3.6.4.8. Permitir a alteração das configurações Módulos da Solução nos clientes de maneira remota;

1.3.6.4.9. Permitir a distribuição remota do agente de proteção para as máquinas;

1.3.6.4.10. Permitir a distribuição remota do software para os servidores que hospedam as máquinas;

1.3.6.4.11. Permitir o gerenciamento do servidor através do protocolo TCP/IP e HTTP;

1.3.6.4.12. A ferramenta de gerência deve suportar a autenticação com segregação de funções, possibilitando a criação de usuários com diferentes níveis de permissão (relatórios, auditoria, configuração);

1.3.6.5. Customização dos relatórios gráficos gerados:

1.3.6.5.1. Exportação dos relatórios para os seguintes formatos: HTML, CSV, PDF;

1.3.6.6. Geração de relatórios que contenham as seguintes informações:

1.3.6.6.1. Os vírus que mais foram detectados;

1.3.6.6.2. As máquinas que mais sofreram infecções em um determinado período de tempo;

1.3.6.6.3. Os usuários que mais sofreram infecções em um determinado período de tempo.

1.3.6.7. Gerenciamento de todos os módulos da suíte:

1.3.6.7.1. Deve possuir log de auditoria, logando todas as ações dos usuários no console de gerenciamento;

1.3.6.8. Políticas/ Configuração:

1.3.6.8.1. A aplicação deve conter um conjunto de políticas pré-configuradas;

1.3.6.8.2. A solução deverá permitir a realização de varreduras por demandas em máquinas que estiverem em estado "offline".

1.3.7. Características de Detecção de Vírus:

1.3.7.1. Precisa ter a capacidade de detectar e bloquear ataques em aplicações Web tais como SQL Injections e Cross Site Scripts. Deverá ainda existir a possibilidade de captura do pacote relacionado ao ataque para fins de investigação do incidente;

1.3.7.2. A solução deve permitir a proteção contra códigos maliciosos através da instalação de agentes, permitindo rastrear ameaças em tempo real, varredura sob demanda e conforme agendamento, possibilitando a tomada de ações distintas para cada tipo de ameaça;

1.3.7.3. A solução deve possibilitar a criação de listas de exclusão, para que o processo do antivírus não execute a varredura de determinados diretórios ou arquivos do SO;



- 1.3.7.4.** A solução deve possibilitar a verificação de ameaças dentro de arquivos compactados, efetuando a limpeza apenas de arquivos maliciosos em casos de detecção;
- 1.3.7.5.** Precisa ter a capacidade de controlar e gerenciar a segurança de múltiplos sistemas operacionais a partir de uma console única;
- 1.3.7.6.** Precisa permitir o gerenciamento das funcionalidades de Firewall, IDS/IPS, Controle de Aplicações, Proteção de Aplicações Web, Inspeção de Logs e Monitoramento de Integridade a partir de uma console única e centralizada;
- 1.3.7.7.** Para efeito de administração, a solução deverá avisar quando um agente se encontra não conectado a sua console de gerenciamento;
- 1.3.7.8.** A solução deve possuir a capacidade de criar políticas de forma global para todas as máquinas, por perfis ou individualmente para cada host.

1.4. CARACTERÍSTICAS TÉCNICAS DA SOLUÇÃO PARA GERENCIAMENTO DE CONECTIVIDADE DE REDES:

- 1.4.1.** A solução deve permitir a configuração de alta disponibilidade nos esquemas ativo-ativo, ativo-passivo e clustering com divisão de carga, sem necessidade de licenciamento adicional;
- 1.4.2.** A solução deve ser capaz de operar sobre os protocolos IPv4 e IPv6, no que for aplicável, para todas as funcionalidades exigidas;
- 1.4.3.** Suportar os protocolos de roteamento OSPF, RIP e BGP, tanto para IPv4 quanto para IPv6;
- 1.4.4.** Suportar uso de roteamento estático;
- 1.4.5.** Suportar VLANs no padrão IEEE 802.1q;
- 1.4.6.** Suportar NAT e PAT, tanto para IPv4 quanto para IPv6;
- 1.4.7.** Permitir a agregação de links via protocolo IEEE 802.3ad;
- 1.4.8.** Permitir a configuração de balanceamento de carga e contingência de links;
- 1.4.9.** Permitir a configuração de DHCP Server e Relay;
- 1.4.10.** Suporte a aplicações multimídia através dos protocolos SIP, H.323, RTP e RTCP;
- 1.4.11.** Permitir a customização da página de bloqueio;
- 1.4.12.** A solução deve suportar Single-Sign-On para Active Directory;
- 1.4.13.** A solução deve vir acompanhada de manual de instruções de forma física, digital ou on-line;
- 1.4.14.** A solução deve permitir a criação de políticas e regras de acesso de maneira integrada, ou seja, em uma única janela, onde possam ser criadas regras que combinem os recursos de firewall, recursos de controle de ameaças, recursos de filtros de URL e recursos de controle de aplicações;
- 1.4.15.** Possuir mecanismo que identifique o conflito de regras e políticas por meio de interface gráfica;
- 1.4.16.** Permitir o uso dos modos stateful e stateless;
- 1.4.17.** Deve suportar PolicyBasedRouting (PBR);
- 1.4.18.** Permitir a criação de regras por meio de usuários, grupos de usuários, portas TCP e UDP, endereços MAC, endereços IPv4 e IPv6, localização geográfica, tipo de dispositivo, horário, protocolos e aplicações;
- 1.4.19.** No que diz respeito a protocolos, considera-se como tal todo e qualquer protocolo localizado na camada de enlace (camada 2 do modelo OSI), rede (camada 3 do modelo OSI) e transporte (camada 4 do modelo OSI);
- 1.4.20.** No que diz respeito a usuários e grupos de usuários, consideram-se como tal usuários e grupos armazenados na base interna da solução, bem como usuários integrados com outras bases por meio do uso de LDAP, Active Directory ou RADIUS;
- 1.4.21.** Permitir o espelhamento de portas (modo sniffer) para fins de monitoramento;
- 1.4.22.** Possuir mecanismos de anti-spoofing de endereços IPv4 e IPv6;
- 1.4.23.** Para a especificação abaixo considera-se malwares todo arquivo que executa ações danosas e atividades maliciosas em um computador ou qualquer dispositivo de rede, como vírus, worms, trojans, ransomwares, bots, spywares, backdoors, rootkits, criptomineradores, etc.
- 1.4.24.** Possuir inspeção de Socket SecureLayer (SSL);



- 1.4.25. Possuir proteção contra-ataques de negação de serviço (DoS);
- 1.4.26. Possuir funcionalidade de detecção avançada de malware “zero-day” baseada em nuvem (Cloud-BasedSandboxing);
- 1.4.27. Deve possuir assinaturas de prevenção de intrusão (IPS);
- 1.4.28. Deve possuir os seguintes mecanismos de inspeção IPS:
 - 1.4.28.1. Análise de padrões de estado de conexão;
 - 1.4.28.2. Análise de decodificação de protocolo;
 - 1.4.28.3. Análise para detecção de anomalias de protocolo;
 - 1.4.28.4. Remontagem de pacotes de TCP;
 - 1.4.28.5. Bloqueio de pacotes malformados;
- 1.4.29. Deve permitir o bloqueio de malwares, vulnerabilidades e exploits conhecidos;
- 1.4.30. Deve prover acesso à base em nuvem permitindo a inspeção de arquivos, realizando a detecção prévia de malwares desconhecidos pela rede;
- 1.4.31. Deve permitir a criação de políticas de IPS e anti-malwares de maneira integrada por zonas de segurança;
- 1.4.32. Permitir a criação de políticas de acesso por meio de cadastros de sites, URLs, trechos de URLs(uso de strings ou expressões regulares), categorias, horários, usuários e grupos de usuários;
- 1.4.33. Possuir base interna de sites/domínios e URLs mantidas e atualizada pelo fabricante, agrupadas por categorias;
- 1.4.34. Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;
- 1.4.35. A base deve possuir pelo menos 60 (sessenta) categorias de sites/domínios;
- 1.4.36. A base deve possuir pelo menos 45 (quarenta e cinco) milhões de sites/domínios cadastrados;
- 1.4.37. A solução deve permitir a customização de categorias em base local, sobrepondo as informações globais;
- 1.4.38. Suportar a inspeção de conteúdo SSL, permitindo a sua integração com políticas de grupo do Active Directory.
- 1.4.39. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer e criar regras de acesso a aplicações, independente de porta e protocolo;
- 1.4.40. Reconhecer pelo menos 1800 (um mil e oitocentas) aplicações diferentes, incluindo, mas não limitado a: peer-to-peer, redes sociais, acesso remoto, VoIP, áudio, vídeo, proxy, mensageiros instantâneos, serviços de armazenamento em nuvem, compartilhamento de arquivos, torrents e e-mail;
- 1.4.41. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;
- 1.4.42. Para tráfego criptografado SSL, deve descriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
- 1.4.43. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;
- 1.4.44. Deve atualizar automaticamente a base de dados de aplicações reconhecidas diretamente do site do fabricante;
- 1.4.45. Permitir a criação de regras por usuário, grupo, aplicação ou categoria de Webfilter;
- 1.4.46. Permitir a definição do tráfego por banda garantida ou máxima;
- 1.4.47. Permitir a criação de políticas de QoS e TrafficShapping por endereço de origem, endereço de destino, aplicação, protocolo, usuários e grupos;
- 1.4.48. Suportar priorização de tráfego usando informações do Tipo de Serviço em IPv4 ou IPv6;
- 1.4.49. Deve possuir suporte a múltiplos fatores de autenticação;
- 1.4.50. Deve possibilitar o acesso a toda infraestrutura interna através da utilização de clientes instalados nas estações;
- 1.4.51. possuir suporte a VPNs e IPSec e SSL;
- 1.4.52. Suportar criptografia AES-128, AES-256 e 3DES;



- 1.4.53. Suportar hash MD5, SHA-256 e SHA-512;
- 1.4.54. Suportar DeadPeerDetection (RFC 3706);
- 1.4.55. A VPN SSL deve possibilitar o acesso a toda infraestrutura interna através da utilização de clientes instalados nas estações;
- 1.4.56. As funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;
- 1.4.57. deve permitir criar políticas de controle de aplicações, IPS, antivírus, antispyware e filtro de URL para tráfego dos clientes remotos conectados na VPN, independente de protocolo(IPSec ou SSL);
- 1.4.58. A solução deve permitir a sua administração de maneira centralizada, sem necessidade de acesso a diferentes sistemas para sua completa configuração;
- 1.4.59. Acesso simultâneo de administradores, integrado via RADIUS ou Active Directory;
- 1.4.60. Acesso remoto criptografado via HTTPS, com interface gráfica Web, e por meio de console SSH;
- 1.4.61. Todas as funções descritas neste edital devem permitir a configuração via interface gráfica web;
- 1.4.62. Permitir o uso de SNMP;
- 1.4.63. Permitir a configuração de alertas e alarmes customizados, bem como seu disparo via e-mail;
- 1.4.64. Permitir a configuração de alertas via e-mail;
- 1.4.65. Permitir o monitoramento de logs em tempo real;
- 1.4.66. Permitir a criação de perfis de acesso à ferramenta;
- 1.4.67. Permitir que os perfis de acesso sejam vinculados a usuários e grupos do Active Directory;
- 1.4.68. Permitir a configuração de relatórios e dashboards customizados;
- 1.4.69. Permitir a visualização do ranking de acessos por usuário, grupo, domínio, site, categoria, aplicação, horário, endereço IPv4 ou IPv6, entre outros;
- 1.4.70. Deve prover relatórios detalhados com análises identificando arquivos como malwares;
- 1.4.71. Deve permitir a exportação de todos os registros gerados pela solução, mesmo em casos de monitoramento, para ferramentas externas através de SYSLOG;
- 1.4.72. Deve permitir identificar graficamente, através de tabela ou mapa, quais os países que mais originaram ou receberam tráfego;
- 1.4.73. Deve permitir identificar graficamente quais as políticas e regras mais utilizadas e a quantidade de tráfego e sessões relacionadas cada política e regra;
- 1.4.74. A solução deve ser nova, sem uso e não estar em estágio de EndofSuppot, EndofSale ou Endof Life ou ainda que tenha previsão anunciada de adentrar em algum destes estágios nos próximos 2(dois) anos a contar da data de publicação do edital;
- 1.4.75. Capacidades globais:**
 - 1.4.75.1. Deve ter capacidade para operar com pelo menos 3 (três) segmentos de redes distintas fisicamente através de portas de rede, permitindo configurar WAN, LAN e DMZ, conforme a necessidade;
 - 1.4.75.2. Possuir suporte a pelo menos 254 (duzentos e cinquenta e quatro) endereços IP em cada interface de rede;
 - 1.4.75.3. Instalação e configuração de toda a solução *remota* com técnicos qualificados;
 - 1.4.75.4. Possuir mecanismo anti-suicídio para a administração remota, evitando que o administrador perca o acesso ao software por uma configuração equivocada;
 - 1.4.75.5. Permitir a conexão simultânea de vários administradores;
 - 1.4.75.6. Deverá permitir backup das configurações local e remoto de forma automatizada;
 - 1.4.75.7. Auditoria de todas as ações realizadas na interface web, logon/logout, visualizações, adições, edições e exclusões;
 - 1.4.75.8. Possibilitar o acesso para interface de configuração e administração via web em português, com total capacidade sobre os recursos e funcionalidades existentes;
 - 1.4.75.9. Garantia e atualizações periódicas do software durante a vigência do contrato de prestação de serviços;



1.4.75.10. Documentação técnica, incluindo manuais de configuração, instalação e operação de toda a solução proposta, todos em português;

1.4.75.11. Licença para cadastramento de **até 150 usuários**.

1.4.76. VPN (Rede Privada Virtual):

1.4.76.1. Deve permitir a criação de túneis VPN (*Virtual Private Network*) dos tipos: *Site-to-Site* (sob o protocolo SSL ou IPSEC) com capacidade para no mínimo 20 (vinte) túneis, *Client-to-site* (sob o protocolo PPTP MSCHAP v2) com capacidade para no mínimo 200 (duzentos) túneis;

1.4.76.2. Permitir a implementação de pelo menos 1.000 (mil) regras de filtro de pacotes, organizadas por grupos com descrição e possibilidade de ativar/inativar determinado grupo de regras;

1.4.76.3. Permitir a implementação de regras orientadas à objetos, tais como: grupo de serviços e grupos de hosts/redes;

1.4.76.4. Possibilitar regras específicas para pelo menos os protocolos GRE, TCP, UDP e ICMP.

1.4.77. Proxy cachê e filtro de conteúdo:

1.4.77.1. Suporte a uso de filtro de conteúdo por domínio, endereço IP, palavra-chave ou extensão de arquivo;

1.4.77.2. Gerenciamento de regras dos filtros de conteúdo por grupos de: *host*, *usuários* e *horários*;

1.4.77.3. Suporte a uso do *Proxy* transparente para o protocolo HTTP, de forma a dispensar a configuração dos browsers das máquinas clientes;

1.4.77.4. Possibilidade de visualizar relatório do conteúdo HTTP (navegação) que fora passado pelo *Proxy*, visualizando o usuário (se autenticado) e/ou host (se transparente);

1.4.77.5. Possibilidade de visualização de relatórios do conteúdo HTTP (navegação) por meses, dias e horários, bem como a listagem dos sites mais acessados, listagem dos maiores arquivos transferidos e números de bytes transferidos por *host*;

1.4.77.6. Possibilidade de visualização, em tempo real, de consumo de banda, por *host* ou sub-rede;

1.4.77.7. Possibilidade de ordenação da visualização em crescente/decrescente do consumo de banda, tempo real, por *host* ou grupo;

1.4.77.8. Autenticação Integrada com *Active Directory*, transparente com SSO (*Single SignOn*);

1.4.77.9. Capacidade de armazenar as atualizações do *Windows Update* e os principais antivírus do mercado, bem como demais softwares a serem informados durante a implementação e/ou durante a vigência do contrato, com o intuito de economizar banda para cada atualização das estações de trabalho.

1.4.78. Balanceamento de carga através de múltiplos links:

1.4.78.1. Suporte à criação de várias tabelas de roteamento, de acordo com cada link de comunicação disponível;

1.4.78.2. Possibilidade de balancear o tráfego para cada link disponível, de acordo com as regras de especificação: por origem, por destino e/ou serviço;

1.4.78.3. Capacidade de proporcionar alta disponibilidade de acesso à Internet e da rede através do balanceamento e da redundância de links dos equipamentos: asseguram a estabilidade na conexão em caso de perda de um dos links ou, ainda, que todos trabalhem para assegurar a continuidade de um determinado serviço.

1.4.79. Controle de banda e QoS:

1.4.79.1. Capacidade de otimizar e priorizar os tráfegos realmente importantes da instituição, como, por exemplo, a priorização de videoconferências;

1.4.79.2. Fornecer serviço de controle de banda e QoS (*Quality of Services*) que permita criar regras para definir a velocidade máxima para determinado tipo de tráfego, baseado na origem, destino ou serviço, bem como por grupos de *hosts*.

1.4.80. Monitoramento de rede e hosts:



1.4.80.1. Fornecer serviço de monitoramento de rede que apresente o tráfego entrante e saínte gerado pelos *hosts* da rede com a especificação do uso dos protocolos;

1.4.82.2. Fornecer serviço de monitoramento de *hosts* que verifica e armazena a disponibilidade de determinados *hosts* cadastrados, com relatório de informações detalhadas como: disponibilidade e latência.

CLÁUSULA II – DA VIGÊNCIA DO CONTRATO

2.1 Este contrato será vigente por 12 (doze) meses, podendo ser prorrogado, se conveniente para a Administração, por iguais e sucessivos períodos, limitada a duração a 48 (quarenta e oito) meses.

CLÁUSULA III – DO PREÇO E DA ENTREGA/IMPLANTAÇÃO

3.1 – Os preços, unitário e total, serão os seguintes:

| Item | Descrição | Quant. | Valor unitário | Valor total |
|------|--|----------|----------------|-------------|
| 1 | Atualização anual das vacinas e software, caso necessário (a partir do segundo ano). | 170 | | |
| 2 | Solução de segurança para servidores (licença de uso para antivírus, somente no primeiro ano). | 3 | | |
| 3 | Aquisição de software para solução endpoint (licença de software, somente no primeiro ano). | 167 | | |
| 4 | Suporte técnico remoto (mensal e permanente durante a vigência do contrato – estimado em 120 horas para 12 meses). | 12 meses | | |
| 5 | Instalação e treinamento remoto inicial, a ser pago uma única vez, no primeiro ano somente. | 1 | | |
| 6 | Solução para gerenciamento de conectividade de redes (mensal e permanente durante a vigência do contrato). | 12 meses | | |

Valor total do contrato: R\$ (valor total).

3.2 Todos os valores ora acordados são entendidos como justos e suficientes para a total execução do objeto deste Contrato, conforme a cláusula primeira deste Instrumento.

3.3 Os itens contratados deverão ser implantados no ambiente computacional da CONTRATANTE localizada na Rua Vale Machado, 1415, CEP 97010.530 – Santa Maria/RS, em dias úteis e em horário de expediente.

3.4 O prazo para implantação e liberação dos itens será de 20 (vinte) dias, a contar da data de assinatura do contrato, podendo ser prorrogado por igual período, desde que apresente justificativa por escrito e previamente autorizada pela autoridade competente para celebrar o contrato.

3.6 Corre por conta do vencedor qualquer prejuízo causado ao patrimônio da Câmara Municipal de Vereadores de Santa Maria por conta de ação de seus empregados quando da execução ou entrega dos serviços contratados.

CLÁUSULA IV - DO RECURSO FINANCEIRO

4.1 Para cobrir as despesas originadas deste contrato, serão utilizadas as dotações das rubricas:



011220001.2.108 – Manutenção das Atividades Administrativas:
3.3.90.40.06 – Locação de Softwares.

CLÁUSULA V – DO PAGAMENTO

5.1 O pagamento será efetuado **em até 05 (cinco) dias úteis** após liquidação da Nota Fiscal, que deverá estar devidamente visada pelo responsável pelo recebimento e conferência do objeto contratado. O pagamento será conforme as etapas já concluídas.

5.1.1 Não haverá, sob qualquer hipótese, qualquer pagamento adiantado à efetiva entrega do objeto contratado.

5.2 Os pagamentos far-se-ão em moeda corrente nacional e serão creditados em nome do Contratado, **após o efetivo cumprimento do objeto contratado devidamente atestado pela fiscalização**, mediante ordem bancária em conta corrente indicada pela Empresa ou por meio de ordem bancária para o pagamento de Nota(s) Fiscal(is), Fatura(s) ou Documento de Cobrança de Valor Jurídico Equivalente, com “código de barras”, uma vez satisfeitas as condições estabelecidas neste Contrato.

5.2.1 Serão descontadas do valor do pagamento as eventuais multas que lhe tenham sido impostas em decorrência de inadimplência contratual.

5.2.2 Qualquer erro ou omissão havido na documentação fiscal ou na fatura será objeto de correção pela empresa e haverá, em decorrência, suspensão do prazo de pagamento até que o problema seja definitivamente regularizado.

5.2.3 A Câmara de Vereadores reserva-se o direito de suspender o pagamento se o objeto for prestado em desacordo com as especificações constantes deste instrumento.

5.3 Tendo sido impostas penalidades ao CONTRATADO das quais não tenha recorrido tempestivamente, ou que já tenham sido objeto de decisão administrativa transitada em julgado, o respectivo valor será descontado do pagamento devido.

5.4 Todo e qualquer pagamento poderá ser sustado, se verificada qualquer das hipóteses a seguir elencadas e enquanto perdurar o ato/fato/omissão que a tiver motivado, sem direito a posterior reajuste, acréscimo, lucros cessantes, indenização, juros e/ou correção monetária:

5.4.1 retardar injustificadamente a execução do objeto da presente licitação;

5.4.2 haver infração à condição ou obrigação estabelecida no edital, contrato ou na proposta apresentada.

5.5 Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido, de alguma forma, para tanto, fica convencionado que a taxa de compensação financeira devida pela Contratante, entre a data do vencimento e o efetivo adimplemento da parcela, é calculada mediante a aplicação da seguinte fórmula:

$$EM = I \times N \times VP$$

5.5.1 Sendo:

EM = Encargos moratórios;

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = Valor da parcela a ser paga.

I = Índice de Compensação Financeira = 0,00016438



5.5.1.1 O Índice de Compensação Financeira (I) mencionado no subitem anterior é apurado da seguinte forma

$I = (TX = \text{Percentual da Taxa Anual} = 6\%)$

$I = (6 / 100) / 365$

$I = 0,00016438$

CLÁUSULA VI – DO REAJUSTE E DO REEQUILÍBRIO ECONÔMICO-FINANCEIRO

6.1 O preço do Contrato poderá ter seu valor mensal reajustado, após o primeiro ano de vigência, utilizando-se o índice acumulado dos últimos 12 (doze) meses do IGP-M – ÍNDICE GERAL DE PREÇOS DO MERCADO (Instituto Brasileiro de Geografia e Estatística).

6.2 Os preços do Contrato poderão ser recompostos, em consonância com o que dispõe o artigo 65, inciso II, alínea “d”, da Lei Federal 8.666/1993.

CLÁUSULA VII – DOS DIREITOS E DAS OBRIGAÇÕES

7.1 Constituem direitos da CONTRATANTE receber o serviço contratado nas exatas condições avençadas, e da CONTRATADA perceber o valor ajustado na forma e no prazo convencionados.

7.2 DAS OBRIGAÇÕES DA CONTRATANTE

7.2.1 Prestar as informações e os esclarecimentos que venham a ser solicitados pela CONTRATADA;

7.2.2 Efetuar o pagamento na forma e no prazo pactuados;

7.2.3 Rejeitar, no todo ou em parte, o objeto que a CONTRATADA entregar fora das especificações constantes neste Contrato.

7.3 DAS OBRIGAÇÕES DA CONTRATADA

7.3.1 Entregar o objeto contratado conforme convencionado, sem qualquer encargo ou despesa para o contratante fora das previsões contratuais;

7.3.2 Cumprir integralmente as obrigações assumidas, especialmente quanto aos prazos estabelecidos e às condições de entrega do objeto;

7.3.3 Utilizar produtos de excelente qualidade para a execução do serviço;

7.3.4 Assumir responsabilidade exclusiva por todos os ônus e tributos, emolumentos, honorários ou despesas incidentais sobre os serviços contratados, bem como cumprir rigorosamente e responsabilizar-se por todas as obrigações trabalhistas, previdenciárias e acidentárias relativas ao pessoal que empregar para a execução dos serviços, inclusive as decorrentes de convenções, acordos ou dissídios coletivos;

7.3.5 Realizar o reparo ou a correção, às suas expensas, dos serviços efetuados em desconformidade com o pactuado, que apresentem vícios, defeitos ou incorreções resultantes de sua execução;

7.3.6 Comunicar à CONTRATANTE qualquer alteração que possa comprometer a manutenção do contrato, nos casos estabelecidos no art. 65 da Lei 8.666/93;

7.3.7 Manter, durante toda a execução do contrato e em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas, de acordo com o previsto no art. 55, XIII da Lei Federal 8.666/93;

7.3.8 Entregar a mesma marca cotada na Proposta de Preços apresentada, **sob pena de recusa do recebimento do item**, nos termos do Art. 55, XI, da Lei Federal nº 8.666/93.

7.3.9 DAS CONDIÇÕES DE MANUTENÇÃO E DO SUPORTE TÉCNICO:

7.3.9.1 O prazo de atendimento começa a ser contado a partir da hora do acionamento do chamado técnico, através de telefone ou e-mail.



7.3.9.2 Tabela de solução do chamado:

| Severidade | Descrição | Métrica | Tempo de solução de atendimento |
|----------------------|---|------------------------|------------------------------------|
| 1 - Urgente | Serviço parado no ambiente de produção, incluindo reposição de peça defeituosa. | Prazo: em horas úteis. | Em até 04 (quatro) horas. |
| 2 - Muito Importante | Erros ou problemas recorrentes que impactam o ambiente de produção. | Prazo: em horas úteis. | Em até 08 (oito) horas. |
| 3 - Importante | Problemas contornáveis. | Prazo: em horas úteis. | Em até 48 (quarenta e oito) horas. |
| 4 - Informação | Consulta técnica, dúvidas em geral, monitoramento, dentre outros. | Prazo: em horas úteis. | Em até 72 (setenta) horas. |

7.3.9.3 Devem ser feitas reuniões gerenciais, mensais ou a critério do CONTRATANTE, para avaliação e acompanhamento dos serviços de manutenção e suporte técnico;

7.3.9.4 Devem ser feitas reuniões técnicas, mensais ou a critério do CONTRATANTE, para planejamento e execução de serviços de manutenção e suporte técnico, com vistas à melhoria do ambiente instalado;

7.3.9.5 Em caso de substituição de equipamento defeituoso, o equipamento substituto deve ser igual ou superior, do mesmo fabricante, em características técnicas;

7.3.9.6 Manter central de suporte técnico, indicando o número de telefone desta ou endereço eletrônico para abertura de chamados;

7.3.10 A CONTRATADA deverá disponibilizar os seguintes canais de atendimento para a abertura de chamados:

7.3.10.1 Sistema de registro de chamados;

7.3.10.2 Telefone;

7.3.10.3 E-mail.

7.3.11 Cada chamado deverá conter, no mínimo, o registro das informações abaixo:

7.3.11.1 Número do chamado;

7.3.11.2 Técnico responsável pelo atendimento;

7.3.11.3 Dados do responsável pela abertura do chamado;

7.3.11.4 Descrição do problema;

7.3.11.5 Situação do chamado (aberto, em atendimento, encerrado, etc.);

7.3.11.6 Severidade (conforme tabela número x);

7.3.11.7 Data e hora de abertura;

7.3.11.8 Histórico do atendimento.

7.3.12 IMPLANTAÇÃO:

7.3.12.1 A CONTRATADA será responsável pela instalação, configuração, atualização com patches do fabricante, integração e testes de todos os produtos fornecidos, inclusive no ambiente atual, de forma a garantir o total funcionamento e operabilidade no ambiente computacional da CONTRATANTE;



7.3.12.2 A CONTRATADA deverá executar todas as atividades (física e lógica) de migração dos serviços que se encontrem em operação, sem ônus para a CONTRATANTE.

7.3.13 RESULTADOS ESPERADOS:

7.3.13.1 Assegurar o provimento de infraestrutura de TI segura e adequada para que a CMVSM continue operacional;

7.3.13.2 Contribuir para garantia de um nível adequado de disponibilidade, autenticidade e confiabilidade das informações produzidas e armazenadas em meios tecnológicos;

7.3.13.3 Oferecer maior agilidade e eficácia no tratamento de incidentes envolvendo endpoints (estações de trabalho notebooks) comprometidos;

7.3.13.4 Evitar, mitigar e conter a propagação de pragas digitais facilitando o tratamento destes incidentes (vírus, malwares, spywares, dentre outros) com a administração centralizada da solução de proteção;

7.3.13.5 Permitir o controle de acesso à rede por dispositivos computacionais, permitindo o gerenciamento destes dispositivos;

7.3.13.6 Gerar melhoria de qualidade do serviço de proteção de endpoints;

7.3.13.7 Aquisição de 170 licenças sendo possível adquirir mais caso necessário pelo mesmo valor das já adquiridas;

7.3.13.8 A solução antivírus deverá gerenciar de forma centralizadas os clientes instalados nas estações de trabalho, utilizando licença de software com função de antivírus, antispymware, firewall, proteção contra intrusos (HIPS);

7.3.13.9 Desinstalação completa de quaisquer soluções similares atualmente existentes nas estações de trabalho da CMVSM;

7.3.13.10 Em resumo os serviços devem ser entregues de modo a prover segurança na camada de usuário, mitigando riscos capazes de impactar a produtividade dos colaboradores da Câmara e degradar o desempenho dos sistemas e redes corporativas;

7.3.13.11 As soluções devem fazer parte do catálogo de produtos comercializados e não ter sido descontinuados;

7.3.13.12 A solução fornecida não deve estar relacionada em listas “endofsale” e “endofsupport” do site do fabricante; Todas as licenças referentes aos sistemas operacionais, bancos de dados e softwares componentes da solução adquirida, inclusive os que forem implantados em ambiente virtualizado, devem estar em nome da CONTRATANTE, legalizado, não sendo admitidas versões “shareware” ou “trial”;

7.3.13.13 Deverão ser fornecidas todas as documentações e manuais técnicos completos necessários à instalação, configuração e operação da solução; A documentação e manuais técnicos deverão estar em português. Deverão ser fornecidos materiais técnicos e manuais em formato digital que permita a importação para base de conhecimento online (Microsoft Word, PDF, HTML etc).

7.3.14 CENTRAL DE ATENDIMENTO:

7.3.14.1 A Contratada deverá manter Central de Atendimento na Web para registro, acompanhamento, resolução de problemas e esclarecimento de dúvidas;

7.3.14.2 Cada atendimento deverá possuir um identificador único para facilitar o acompanhamento das soluções;

7.3.14.3 O acesso à Central de Atendimento disponível para atender as demandas da Câmara de Vereadores deverá estar disponível pelos canais: por ligação telefônica gratuita (0800), via Central na Web e por correio eletrônico (e-mail).

7.3.14.4 A Central de Atendimento na Web deverá possibilitar pelo menos as seguintes funcionalidades:

a) Abertura / Acompanhamento de Chamados, regidos pelo SLA contratado;

b) Documentações do Cliente (manuais procedimentos e outros arquivos de interesse do contrato);

c) Emissão / Reimpressão de faturas e pagamentos; e

d) Impressão Notas Fiscais Emitidas.



7.3.15 CONDIÇÕES GERAIS PARA PRESTAÇÃO DE SERVIÇOS:

7.3.15.1 Os serviços deverão estar disponíveis durante 24 horas do dia, nos 7 dias da semana;

7.3.15.2 Toda a solução que contemplam os serviços acima deverá incluir Hardware, Software, Serviços de instalação e suporte técnico durante as 24 (vinte e quatro) horas do dia nos 365 (trezentos e sessenta e cinco) dias do ano, de forma ininterrupta;

7.3.15.3 Todos os materiais, respectivos acessórios e cabeamentos fornecidos deverão ser novos, e em perfeitas condições para sua instalação e operação imediata;

7.3.15.4 Em caso de dano ou paralisação parcial ou total do equipamento por decorrência da sua operação normal, caberá à empresa contratada a manutenção ou sua substituição por outro appliance de mesmas características técnicas e também recuperação das configurações, sem quaisquer ônus adicional.

CLÁUSULA VIII – DA INEXECUÇÃO DO CONTRATO

8.1 A CONTRATADA reconhece os direitos da CONTRATANTE em caso de rescisão administrativa, previstos no art. 77, da Lei Federal nº 8.666/93 e suas alterações.

CLÁUSULA IX – DA RESCISÃO

9.1 Este contrato poderá ser rescindido:

9.1.1 Por ato unilateral da CONTRATANTE, nos casos dos incisos I a XII e XVII do art. 78 da Lei 8.666/93, de 21 de junho de 1993;

9.1.2 Amigavelmente, por acordo entre as partes reduzido a termo no processo de licitação, desde que haja conveniência para a CONTRATANTE;

9.1.3 Judicialmente, nos termos da legislação aplicável.

9.2 A rescisão deste contrato implicará retenção de créditos decorrentes da contratação, até o limite dos prejuízos causados ao CONTRATANTE, bem como na assunção dos serviços pela CONTRATANTE na forma que a mesmo determinar.

CLÁUSULA X – DAS PENALIDADES E DAS MULTAS

10.1 Pelo descumprimento, parcial ou total, das condições previstas na proposta ou no contrato, a CONTRATANTE poderá aplicar à CONTRATADA as seguintes sanções previstas no art. 87, da Lei 8.666/93, sem prejuízo da responsabilização civil e penal cabíveis:

10.1.1 Advertência formal, por intermédio do setor competente, quando ocorrer descumprimento de cláusulas contratuais que não justifiquem a aplicação de penalidade mais grave;

10.1.2 Multa de Mora equivalente a 0,5 % (meio por cento) sobre o valor global do contrato, para cada dia de atraso no início da prestação do serviço.

10.1.2.1 A multa de que trata o item anterior não impedirá a rescisão unilateral do contrato pela CONTRATANTE, na forma dos artigos 77 e seguintes da Lei 8.666/1993;

10.1.3 Multa sobre o valor total atualizado no contrato:

10.1.3.1 De até 2% (dois por cento) pelo descumprimento de cláusula contratual ou norma da legislação pertinente;

10.1.3.2 De até 30% (trinta por cento) nos casos de inexecução total ou parcial do contrato.



10.1.4 Suspensão do direito de licitar e contratar com a Administração, por período de até 24 (vinte e quatro) meses, de acordo com a natureza e a gravidade da falta, sem prejuízo da aplicação de multa, obedecida a seguinte graduação:

10.1.4.1 Após advertência formal e cobrança de multa, ser reincidente, sem justificativa, nas penalidades avençadas neste Contrato: Prazo da Suspensão de até 12 (doze) meses;

10.1.4.2 Não iniciar a execução da prestação do serviço no prazo estabelecido, desobedecendo à solicitação por escrito da CONTRATANTE: Prazo da Suspensão até 24 (vinte e quatro) meses.

10.1.5 Declaração de Inidoneidade para licitar e contratar com a Administração Pública, em função de falta de natureza grave, sem prejuízo de multas incidentes, publicada no Diário Oficial do Estado;

10.1.6 Outras penalidades previstas nas Leis Federais nº 8.666/1993 e 10.520/2002.

10.2 A aplicação de qualquer das penalidades previstas realizar-se-á mediante prévio e regular processo administrativo, que assegurará, absolutamente, o contraditório e a ampla defesa ao licitante/adjudicatário, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente na Lei nº 9.784, de 1999.

10.3 As penalidades previstas neste instrumento contratual poderão deixar de ser aplicadas, total ou parcialmente, a critério da CONTRATANTE, se entender como relevantes as justificativas apresentadas pela CONTRATADA.

10.4 Eventuais multas aplicadas deverão ser liquidadas simultaneamente com o pagamento da parcela vinculada ao evento cujo descumprimento deu origem à aplicação da penalidade;

10.4.1 Caso a multa não seja recolhida nas condições acima descritas, será descontada do pagamento da parcela vinculada ao evento cujo descumprimento deu origem à aplicação da penalidade.

CLÁUSULA XI – DA EFICÁCIA

11.1 O presente Contrato somente terá eficácia após a publicação da respectiva súmula no Diário Oficial do Estado.

CLÁUSULA XII – DO FISCAL DO CONTRATO

12.1 Fica designado o “**GESTORCONTRATO**” como Gestor do Contrato e o Servidor “**FISCALCONTRATO**” como Fiscal do Contrato.

CLÁUSULA XIII: DA LEGISLAÇÃO APLICÁVEL E DA VINCULAÇÃO DO CONTRATO

13.1 Este Contrato rege-se pela legislação mencionada no seu Preâmbulo, inclusive nos casos omissos, vinculando-se às instruções contidas no Edital do Pregão nº 07/2019 e à proposta apresentada pela CONTRATADA durante o Processo Licitatório nº 51/2019.

CLÁUSULA XIV – DA SUBCONTRATAÇÃO, FUSÃO, CISÃO OU INCORPORAÇÃO

14.1 É vedada a subcontratação total ou parcial do objeto, a associação do contratado com outrem, a cessão ou transferência (total ou parcial), bem como a fusão, cisão ou incorporação, constituindo motivos para rescisão do contrato.

CLÁUSULA XV – DO FORO



Câmara Municipal de Vereadores de Santa Maria
Centro Democrático Adelmo Simas Genro

15.1 Fica eleito o **Foro da Comarca de Santa Maria - RS**, com exclusão de qualquer outro, por mais privilegiado que seja, para dirimir dúvidas ou questões oriundas do presente Contrato.

15.2 E, por estarem justos e contratados, firmam o presente em 03 (três) vias de igual teor e forma, na presença de duas testemunhas.

Santa Maria, ____ de _____ de 2019.

PRESIDENTE CMVSM

RESPONSÁVEL LEGAL
EMPRESA CONTRATADA

TESTEMUNHAS:



ANEXO II - TERMO DE REFERÊNCIA – PREGÃO PRESENCIAL Nº 07/2019

1. OBJETO

- 1.1. Contratação de empresa capacitada para prestar serviço de solução para gerenciamento de conectividade de redes e prevenção de ameaças com suporte remoto para até 180 usuários;
- 1.2. Aquisição de licença de Software para solução endpoint e para solução de segurança para servidores (licença de uso para antivírus);
- 1.3. Suporte técnico remoto (estimada em 120 horas para 12 meses) para atualização e implantação da solução antivírus para endpoints e servidores;
- 1.4. Atualização anual das vacinas das soluções;
- 1.5. Instalação e treinamento remoto inicial;
- 1.6. Cabe salientar que a descrição dos dispositivos aqui propostos, é uma sugestão de hardware e software, baseados em tecnologias atuais e de qualidade mínima, que permitem a várias empresas participarem de licitação.

2. SOLUÇÃO DE SEGURANÇA

2.1. Contratação de empresa especializada no fornecimento de solução integrada de segurança e prevenção de ameaças composta por antivírus empresarial + appliance firewall que deverão trabalhar juntas para melhor desempenho, incluindo serviço de instalação, suporte técnico online, repasse de conhecimento hands-on, garantia e atualização durante a vigência do contrato, conforme condições, quantidades, exigências e estimativas descritas no termo. Contratação de Solução de segurança para a rede com **appliance firewall** e proteção da infraestrutura **com proteção avançada dos endpoints**.

2.2. Justificativa da locação do appliance firewall:

- 2.2.1. Processo de compra de natureza lenta caso precise reparos ou substituição;
- 2.2.2. Evolução constante da tecnologia em curto espaço de tempo que pode tornar obsoleto o equipamento dentro do prazo do contrato;
- 2.2.3. Dificuldades para comprar outro, por já ter adquirido um, caso a instituição tenha um aumento da demanda e precise de um equipamento mais potente.

3. JUSTIFICATIVA

3.1. A Solução de Rede Local abrange a contratação de soluções de segurança, como Firewall, Proxy, entre outras, justificadas para assegurar que não tenha, por exemplo, utilização indevida das estruturas por elementos externos ou internos, indisponibilidade, acesso a informações não pertinentes ao uso desta Casa Legislativa, acesso oriundo de meio externo a informações classificadas como sigilosas e armazenadas nos servidores e computadores. Essas soluções também garantem a integridade das informações e restringem o acesso para que somente as pessoas autorizadas possam coletar, alterar ou remover configurações dos elementos de rede. Ainda para que se tenha registro de acesso aos sites pelos usuários.

4. CARACTERÍSTICAS GERAIS DA SOLUÇÃO PARA GERENCIAMENTO DE CONECTIVIDADE DE REDES

- 4.1. A solução deverá ser composta por 1 appliance física contendo todos os softwares necessários para o seu correto e perfeito funcionamento, monitoramento e gerenciamento;
- 4.2. A solução deve ser de um único fabricante e possuir arquitetura de hardware dedicada (não x86);
- 4.3. A solução deverá suportar, com todos os serviços internos ativos (antivírus, firewall, VPN, IPS, etc.), um link de 100Mbps dedicado e com cerca de 300 dispositivos conectados sem degradação de performance do link; além disso suportar (fazendo substituição/upgrade de equipamento se



necessário), dentro de 3 anos, um possível incremento do link dedicado para 200Mbps dedicado e aumento do número de dispositivos conectados para 600 sem degradação do link também;

4.4. Cada appliance deve atender no mínimo aos seguintes requisitos (características de hardware e performance):

4.4.1. Throughput de, no mínimo, 4.4 Gbps com a funcionalidade de firewall habilitada para tráfego IPv4 e IPv6, independentemente do tamanho do pacote;

4.4.2. Suporte a, no mínimo, 2M conexões simultâneas;

4.4.3. Suporte a, no mínimo, 30.000 novas conexões por segundo;

4.4.4. Throughput de, no mínimo, 4 Gbps de VPN IPsec;

4.4.5. Estar licenciado para ou suportar sem o uso de licença, 2K túneis de VPN IPSEC Site-to-Site simultâneos;

4.4.6. Estar licenciado para ou suportar sem o uso de licença, 10K túneis de clientes VPN IPSEC simultâneos;

4.4.7. Throughput de, no mínimo, 200 Mbps de VPN SSL;

4.4.8. Estar licenciado para no mínimo, 5K clientes de VPN SSL simultâneos;

4.4.9. Suportar no mínimo 500 Mbps de throughput de IPS;

4.4.10. Suportar no mínimo 130 Mbps de throughput de Inspeção SSL;

4.4.11. Throughput de, no mínimo, 360 Mbps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS, Antivírus e Antispyware. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o menor valor será aceito;

4.4.12. Possuir ao menos 8 interfaces 1Gbps Ethernet RJ45;

4.4.13. Possuir ao menos 2 interfaces 1Gbps Ethernet SFP;

4.4.14. Estar licenciado e/ou ter incluído sem custo adicional, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance;

4.4.15. Suporte a, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance;

4.4.16. Possuir armazenamento interno de no mínimo 420 GB para armazenar logs;

4.4.17. Para fim de aferição das taxas definidas nos itens 4.4.1. a 4.4.19., considerar-se-ão apenas informações contidas em documentos de domínio público do fabricante;

4.4.18. A solução deve ter altura máxima de 2U;

4.4.19. A solução deve funcionar em 110-240V 50-60Hz, definido automaticamente pelo aparelho.

4.5. A solução deverá estar instalada e configurada no prazo de 20 dias a partir da data de assinatura do contrato.

5. CARACTERÍSTICAS DA SOLUÇÃO ANTIVÍRUS:

5.1. Suporte total aos sistemas operacionais baseados na plataforma Windows:

5.1.1. Windows 2012 Server Standard;

5.1.2. Suporte total a Windows 7, Windows 8, Windows 10;

5.1.3. Suporte total a plataforma 32 e 64 bits.

5.2. Todas as funcionalidades deste item devem ser ativadas por agente único que facilite a instalação, a configuração e o gerenciamento.

5.3. Rastreamento em tempo real, para arquivos durante entrada e saída (gravação e leitura), com as seguintes opções:

5.3.1. Negar acesso ao arquivo infectado e prosseguir;

5.3.2. Limpar o arquivo;

5.3.3. Apagar o arquivo infectado;

5.3.4. Mover o arquivo infectado para área de segurança (quarentena);



- 5.3.5.** Rastreamento manual com interface Windows, customizável, com opção de limpeza;
- 5.3.6.** Permitir diferentes configurações de varredura em tempo real baseando-se em processos de baixo ou alto risco, tornando assim o desempenho do produto mais estável;
- 5.3.7.** Rastreamento em tempo real dos processos em memória, para a captura de vírus que são executados em memória sem a necessidade de escrita de arquivo;
- 5.3.8.** Detecção de programas maliciosos como spyware, programas de propaganda, ferramentas como password crackers, etc.;
- 5.3.9.** Programação de atualizações automáticas das definições de vírus, a partir de local predefinido da rede, ou de site da Internet, com frequência (no mínimo diária) e horários definidos pelo administrador;
- 5.3.10.** Permitir atualização incremental da lista de definições de vírus;
- 5.3.11.** Opção de downgrade de vacina via console de gerenciamento.

5.4. Programação de rastreamentos automáticos do sistema com as seguintes opções:

- 5.4.1.** Escopo: Todos os drives locais, drives específicos, ou pastas específicas;
- 5.4.2.** Ação: Somente alertas, limpar automaticamente, apagar automaticamente, renomear automaticamente, ou mover automaticamente para área de segurança (quarentena);
- 5.4.3.** Frequência: Horária, diária, semanal, mensal;
- 5.4.4.** Exclusões: Pastas ou arquivos que não devem ser rastreados;
- 5.4.5.** Gerar registro (log) dos eventos de vírus em arquivo e local definido pelo administrador, com limite de tamanho opcional;
- 5.4.6.** Gerar notificações de eventos de vírus através de alerta na rede;
- 5.4.7.** Detectar, analisar e eliminar, automaticamente e em tempo real, programas maliciosos em:
- 5.4.8.** Processos em execução em memória principal (RAM);
- 5.4.9.** Arquivos criados, copiados, renomeados, movidos ou modificados, inclusive em sessões de linha de comando (DOS ou shell) abertas pelo usuário;
- 5.4.10.** Arquivos compactados automaticamente, em pelo menos nos seguintes formatos: ZIP, EXE, ARJ, MIME/UU, Microsoft CAB, Microsoft Compress;
- 5.4.11.** Arquivos recebidos por meio de programas de comunicação instantânea (MSN Messenger, Yahoo Messenger, Google Talk, dentre outros);
- 5.4.12.** Capacidade de finalizar processos com nomes de vírus ou nomes relacionados;
- 5.4.13.** Possibilidade de reparar o registro do sistema após eliminação de epidemia;
- 5.4.14.** Permitir bloqueio de portas;
- 5.4.15.** Permitir criação de regras baseadas em processos de sistema;
- 5.4.16.** Permitir o bloqueio de compartilhamentos da máquina em caso de epidemia;
- 5.4.17.** Possuir proteção contra estouro de buffer;
- 5.4.18.** Capacidade de retomar atualizações do ponto onde foram interrompidas em caso de perda de conexão, sem necessidade de reinício de todo o processo;
- 5.4.19.** Detecção de cookies potencialmente indesejáveis no sistema;
- 5.4.20.** O sistema de antispware deve estar totalmente integrado ao software antivírus utilizando a mesma biblioteca de definições de vírus e demais ameaças;
- 5.4.21.** O sistema deve estar integrado ao console de gerenciamento de segurança de sistemas, que também gerencia antivírus antispware, antispam e controle de acesso à rede, possibilitando uma única e simples interface para gerenciar toda uma solução de segurança. Não deve ser instalado nenhum software adicional a console de gerenciamento para permitir o controle integrado;
- 5.4.22.** Oferecer proteção avançada de sistemas contra ameaças tais como ataques remotos de injeção de SQL ou HTTP;
- 5.4.23.** Trabalhar no modo de quarentena permitindo a verificação pelo software de gerenciamento se o cliente está trabalhando com políticas antigas e versões desatualizadas, neste caso, o cliente é bloqueado a uma área de quarentena, limitando a acesso a rede desta estação;
- 5.4.24.** Capacidade de detectar e bloquear tentativas de invasão;
- 5.4.25.** Possuir instalação "silenciosa";



- 5.4.26. Possibilidade de varredura de portas das estações de trabalho;
- 5.4.27. Possuir sistema contra vulnerabilidades de sistemas operacionais e aplicativos (principalmente Microsoft), antes de ser aplicada a correção dessas falhas nos endpoints;
- 5.4.28. Sistema de Proteção para sistemas contra vulnerabilidades não corrigidas;
- 5.4.29. Sistema de proteção contra ameaças mesmo se ainda não tiverem instalado uma correção do fornecedor que lide com uma vulnerabilidade conhecida.

5.5. Características do Módulo para Gerenciamento da Solução:

- 5.5.1. Programação de atualizações automáticas das listas de definições de vírus, a partir de local predefinido da rede, ou de site seguro da Internet, com frequência (no mínimo diária) e horários definidos pelo administrador da solução;
- 5.5.2. Permitir atualização incremental da lista de definições de vírus;
- 5.5.3. Atualização automática do engine do programa de proteção a partir de localização na rede local ou na Internet, a partir de fonte autenticável;
- 5.5.4. Permitir o retorno (rollback) das atualizações das listas de definições de vírus e motores de varreduras.
- 5.5.5. Gerar registro (log) dos eventos de vírus em arquivo e local definido pelo administrador da solução, com limite de tamanho opcional;
- 5.5.6. Permitir proteção das configurações da solução instalada na estação de trabalho através de senha ou controle de acesso, em ambos os casos, controlada por política gerenciada pela console de administração da solução completa;
- 5.5.7. Permitir o gerenciamento do servidor a partir de console tipo web, com acesso via https, instalada em outra máquina;
- 5.5.8. Permitir a instalação do Antivírus nos clientes a partir de um único servidor;
- 5.5.9. Permitir a criação de tarefas de atualização, verificação de vírus e upgrades em períodos de tempo pré-determinados, na inicialização do Sistema Operacional ou no Logon na rede;
- 5.5.10. Suporte a múltiplos usuários, com diferentes níveis de acesso e permissões aos produtos gerenciados;
- 5.5.11. Forçar a instalação do software Antivírus nos clientes;
- 5.5.12. Caso o cliente desinstale o software Antivírus, o mesmo deverá ser reinstalado, quando o agente verificar o ocorrido;
- 5.5.13. Customização dos relatórios gráficos gerados;
- 5.5.14. Geração de relatórios que contenham as seguintes informações:
 - 5.5.14.1. Máquinas com a lista de definições de vírus desatualizada;
 - 5.5.14.2. Qual a versão do software instalado em cada máquina;
 - 5.5.14.3. Os vírus que mais foram detectados;
 - 5.5.14.4. As máquinas que mais sofreram infecções em um determinado período de tempo;
 - 5.5.14.5. Os usuários que mais sofreram infecções em um determinado período de tempo;
 - 5.5.14.6. Gerenciamento de todos os módulos da suíte.

5.6. Característica da Solução Antivírus para Servidor:

- 5.6.1. A solução deverá permitir a sua implantação atendendo as seguintes características:
 - 5.6.1.1. Multi-Plataforma, atuando para realizar o rastreamento em tempo real, por demanda e agendado de malwares, através da utilização de uma máquina com a solução Antivírus instalada efetuando todas as análises da estrutura, sem a necessidade de qualquer integração com agentes externos ou a instalação de clientes Antivírus em cada uma das máquinas.
- 5.6.2. Sistemas Operacionais Suportados para o servidor de varredura Offload:
 - 5.6.2.1. Windows 2012 Server Standard;
- 5.6.3. Sistemas Operacionais Suportados nas máquinas a serem varridas em busca de ameaças:
 - 5.6.3.1. Windows 7 (32 ou 64 bits);
 - 5.6.3.2. Windows 8 Beta (32 ou 64 bits);
 - 5.6.3.3. Windows 10 (32 ou 64 bits).



5.6.4. Console de Gerência da Solução:

5.6.4.1. Deve dar suporte à instalação em um servidor nas plataformas Windows 2012 Server Standard;

5.6.4.2. O Gerenciador deve trabalhar em modo Cluster;

5.6.4.3. O gerenciador deve prover ferramentas de Backup e Restore;

5.6.4.4. A ferramenta de gerência deve possibilitar autenticação externa integrada a estrutura LDAP;

5.6.4.5. A ferramenta de gerência deve suportar o gerenciamento de políticas de senha de autenticação na console;

5.6.4.6. A solução de gerenciamento deve permitir acesso a sua console via web;

5.6.4.7. Implementação de Dashboard com medição do nível de atualização do ambiente e o nível de cumprimento de política de segurança previamente definida;

5.6.4.8. Permitir a alteração das configurações Módulos da Solução nos clientes de maneira remota;

5.6.4.9. Permitir a distribuição remota do agente de proteção para as máquinas;

5.6.4.10. Permitir a distribuição remota do software para os servidores que hospedam as máquinas;

5.6.4.11. Permitir o gerenciamento do servidor através do protocolo TCP/IP e HTTP;

5.6.4.12. A ferramenta de gerência deve suportar a autenticação com segregação de funções, possibilitando a criação de usuários com diferentes níveis de permissão (relatórios, auditoria, configuração).

5.6.5. Customização dos relatórios gráficos gerados:

5.6.5.1. Exportação dos relatórios para os seguintes formatos: HTML, CSV, PDF.

5.6.6. Geração de relatórios que contenham as seguintes informações:

5.6.6.1. Os vírus que mais foram detectados;

5.6.6.2. As máquinas que mais sofreram infecções em um determinado período de tempo;

5.6.6.3. Os usuários que mais sofreram infecções em um determinado período de tempo.

5.6.7. Gerenciamento de todos os módulos da suíte:

5.6.7.1. Deve possuir log de auditoria, logando todas as ações dos usuários no console de gerenciamento.

5.6.8. Políticas/ Configuração:

5.6.8.1. A aplicação deve conter um conjunto de políticas pré-configuradas;

5.6.8.2. A solução deverá permitir a realização de varreduras por demandas em máquinas que estiverem em estado "offline".

5.7. Características de Detecção de Vírus:

5.7.1. Precisa ter a capacidade de detectar e bloquear ataques em aplicações Web tais como SQL Injections e Cross Site Scripts. Deverá ainda existir a possibilidade de captura do pacote relacionado ao ataque para fins de investigação do incidente;

5.7.2. A solução deve permitir a proteção contra códigos maliciosos através da instalação de agentes, permitindo rastrear ameaças em tempo real, varredura sob demanda e conforme agendamento, possibilitando a tomada de ações distintas para cada tipo de ameaça;

5.7.3. A solução deve possibilitar a criação de listas de exclusão, para que o processo do antivírus não execute a varredura de determinados diretórios ou arquivos do SO;

5.7.4. A solução deve possibilitar a verificação de ameaças dentro de arquivos compactados, efetuando a limpeza apenas de arquivos maliciosos em casos de detecção;

5.7.5. Precisa ter a capacidade de controlar e gerenciar a segurança de múltiplos sistemas operacionais a partir de uma console única;

5.7.6. Precisa permitir o gerenciamento das funcionalidades de Firewall, IDS/IPS, Controle de Aplicações, Proteção de Aplicações Web, Inspeção de Logs e Monitoramento de Integridade a partir de uma console única e centralizada;

5.7.7. Para efeito de administração, a solução deverá avisar quando um agente se encontra não conectado a sua console de gerenciamento;

5.7.8. A solução deve possuir a capacidade de criar políticas de forma global para todas as máquinas, por profiles ou individualmente para cada host.



5.8 Planilha de quantitativos:

| Item | Descrição | Quantidade |
|------|--|------------|
| 1 | Atualização anual das vacinas e software, caso necessário (a partir do segundo ano). | 170 |
| 2 | Solução de segurança para servidores (licença de uso para antivírus, somente no primeiro ano). | 3 |
| 3 | Aquisição de software para solução endpoint (licença de software, somente no primeiro ano). | 167 |
| 4 | Suporte técnico remoto (mensal e permanente durante a vigência do contrato – estimado em 120 horas para 12 meses). | 12 meses |
| 5 | Instalação e treinamento remoto inicial, a ser pago uma única vez, no primeiro ano somente. | 1 |
| 6 | Solução para gerenciamento de conectividade de redes (mensal e permanente durante a vigência do contrato). | 12 meses |

6. CARACTERÍSTICAS TÉCNICAS DA SOLUÇÃO PARA GERENCIAMENTO DE CONECTIVIDADE DE REDES:

- 6.1. A solução deve permitir a configuração de alta disponibilidade nos esquemas ativo-ativo, ativo-passivo e clustering com divisão de carga, sem necessidade de licenciamento adicional;
- 6.2. A solução deve ser capaz de operar sobre os protocolos IPv4 e IPv6, no que for aplicável, para todas as funcionalidades exigidas;
- 6.3. Suportar os protocolos de roteamento OSPF, RIP e BGP, tanto para IPv4 quanto para IPv6;
- 6.4. Suportar uso de roteamento estático;
- 6.5. Suportar VLANs no padrão IEEE 802.1q;
- 6.6. Suportar NAT e PAT, tanto para IPv4 quanto para IPv6;
- 6.7. Permitir a agregação de links via protocolo IEEE 802.3ad;
- 6.8. Permitir a configuração de balanceamento de carga e contingência de links;
- 6.9. Permitir a configuração de DHCP Server e Relay;
- 6.10. Suporte a aplicações multimídia através dos protocolos SIP, H.323, RTP e RTCP;
- 6.11. Permitir a customização da página de bloqueio;
- 6.12. A solução deve suportar Single-Sign-On para Active Directory;
- 6.13. A solução deve vir acompanhada de manual de instruções de forma física, digital ou on-line;
- 6.14. A solução deve permitir a criação de políticas e regras de acesso de maneira integrada, ou seja, em uma única janela, onde possam ser criadas regras que combinem os recursos de firewall, recursos de controle de ameaças, recursos de filtros de URL e recursos de controle de aplicações;
- 6.15. Possuir mecanismo que identifique o conflito de regras e políticas por meio de interface gráfica;
- 6.16. Permitir o uso dos modos stateful e stateless;
- 6.17. Deve suportar PolicyBasedRouting (PBR);
- 6.18. Permitir a criação de regras por meio de usuários, grupos de usuários, portas TCP e UDP, endereços MAC, endereços IPv4 e IPv6, localização geográfica, tipo de dispositivo, horário, protocolos e aplicações;
- 6.19. No que diz respeito a protocolos, considera-se como tal todo e qualquer protocolo localizado na camada de enlace (camada 2 do modelo OSI), rede (camada 3 do modelo OSI) e transporte (camada 4 do modelo OSI);
- 6.20. No que diz respeito a usuários e grupos de usuários, consideram-se como tal usuários e grupos armazenados na base interna da solução, bem como usuários integrados com outras bases por meio do uso de LDAP, Active Directory ou RADIUS;
- 6.21. Permitir o espelhamento de portas (modo sniffer) para fins de monitoramento;



- 6.22.** Possuir mecanismos de anti-spoofing de endereços IPv4 e IPv6;
- 6.23.** Para a especificação abaixo considera-se malwares todo arquivo que executa ações danosas e atividades maliciosas em um computador ou qualquer dispositivo de rede, como vírus, worms, trojans, ransomwares, bots, spywares, backdoors, rootkits, criptomineradores, etc.
- 6.24.** Possuir inspeção de Socket SecureLayer (SSL);
- 6.25.** Possuir proteção contra-ataques de negação de serviço (DoS);
- 6.26.** Possuir funcionalidade de detecção avançada de malware “zero-day” baseada em nuvem (Cloud-BasedSandboxing);
- 6.27.** Deve possuir assinaturas de prevenção de intrusão (IPS);
- 6.28.** Deve possuir os seguintes mecanismos de inspeção IPS:
 - 6.28.1.** Análise de padrões de estado de conexão;
 - 6.28.2.** Análise de decodificação de protocolo;
 - 6.28.3.** Análise para detecção de anomalias de protocolo;
 - 6.28.4.** Remontagem de pacotes de TCP;
 - 6.28.5.** Bloqueio de pacotes malformados;
- 6.29.** Deve permitir o bloqueio de malwares, vulnerabilidades e exploits conhecidos;
- 6.30.** Deve prover acesso à base em nuvem permitindo a inspeção de arquivos, realizando a detecção prévia de malwares desconhecidos pela rede;
- 6.31.** Deve permitir a criação de políticas de IPS e anti-malwares de maneira integrada por zonas de segurança;
- 6.32.** Permitir a criação de políticas de acesso por meio de cadastros de sites, URLs, trechos de URLs(uso de strings ou expressões regulares), categorias, horários, usuários e grupos de usuários;
- 6.33.** Possuir base interna de sites/domínios e URLs mantidas e atualizada pelo fabricante, agrupadas por categorias;
- 6.34.** Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;
- 6.35.** A base deve possuir pelo menos 60 (sessenta) categorias de sites/domínios;
- 6.36.** A base deve possuir pelo menos 45 (quarenta e cinco) milhões de sites/domínios cadastrados;
- 6.37.** A solução deve permitir a customização de categorias em base local, sobrepondo as informações globais;
- 6.38.** Suportar a inspeção de conteúdo SSL, permitindo a sua integração com políticas de grupo do Active Directory.
- 6.39.** Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer e criar regras de acesso a aplicações, independente de porta e protocolo;
- 6.40.** Reconhecer pelo menos 1800 (um mil e oitocentas) aplicações diferentes, incluindo, mas não limitado a: peer-to-peer, redes sociais, acesso remoto, VoIP, áudio, vídeo, proxy, mensageiros instantâneos, serviços de armazenamento em nuvem, compartilhamento de arquivos, torrents e e-mail;
- 6.41.** Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;
- 6.42.** Para tráfego criptografado SSL, deve decriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
- 6.43.** Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;
- 6.44.** Deve atualizar automaticamente a base de dados de aplicações reconhecidas diretamente do site do fabricante;
- 6.45.** Permitir a criação de regras por usuário, grupo, aplicação ou categoria de Webfilter;
- 6.46.** Permitir a definição do tráfego por banda garantida ou máxima;
- 6.47.** Permitir a criação de políticas de QoS e TrafficShapping por endereço de origem, endereço de destino, aplicação, protocolo, usuários e grupos;
- 6.48.** Suportar priorização de tráfego usando informações do Tipo de Serviço em IPv4 ou IPv6;



- 6.49. Deve possuir suporte a múltiplos fatores de autenticação;
- 6.50. Deve possibilitar o acesso a toda infraestrutura interna através da utilização de clientes instalados nas estações;
- 6.51. possuir suporte a VPNs e IPsec e SSL;
- 6.52. Suportar criptografia AES-128, AES-256 e 3DES;
- 6.53. Suportar hash MD5, SHA-256 e SHA-512;
- 6.54. Suportar DeadPeerDetection (RFC 3706);
- 6.55. A VPN SSL deve possibilitar o acesso a toda infraestrutura interna através da utilização de clientes instalados nas estações;
- 6.56. As funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;
- 6.57. deve permitir criar políticas de controle de aplicações, IPS, antivírus, antispymware e filtro de URL para tráfego dos clientes remotos conectados na VPN, independente de protocolo(IPsec ou SSL);
- 6.58. A solução deve permitir a sua administração de maneira centralizada, sem necessidade de acesso a diferentes sistemas para sua completa configuração;
- 6.59. Acesso simultâneo de administradores, integrado via RADIUS ou Active Directory;
- 6.60. Acesso remoto criptografado via HTTPS, com interface gráfica Web, e por meio de console SSH;
- 6.61. Todas as funções descritas neste edital devem permitir a configuração via interface gráfica web;
- 6.62. Permitir o uso de SNMP;
- 6.63. Permitir a configuração de alertas e alarmes customizados, bem como seu disparo via e-mail;
- 6.64. Permitir a configuração de alertas via e-mail;
- 6.65. Permitir o monitoramento de logs em tempo real;
- 6.66. Permitir a criação de perfis de acesso à ferramenta;
- 6.67. Permitir que os perfis de acesso sejam vinculados a usuários e grupos do Active Directory;
- 6.68. Permitir a configuração de relatórios e dashboards customizados;
- 6.69. Permitir a visualização do ranking de acessos por usuário, grupo, domínio, site, categoria, aplicação, horário, endereço IPv4 ou IPv6, entre outros;
- 6.70. Deve prover relatórios detalhados com análises identificando arquivos como malwares;
- 6.71. Deve permitir a exportação de todos os registros gerados pela solução, mesmo em casos de monitoramento, para ferramentas externas através de SYSLOG;
- 6.72. Deve permitir identificar graficamente, através de tabela ou mapa, quais os países que mais originaram ou receberam tráfego;
- 6.73. Deve permitir identificar graficamente quais as políticas e regras mais utilizadas e a quantidade de tráfego e sessões relacionadas cada política e regra;
- 6.74. A solução deve ser nova, sem uso e não estar em estágio de EndofSuppot, EndofSale ou Endof Life ou ainda que tenha previsão anunciada de adentrar em algum destes estágios nos próximos 2(dois) anos a contar da data de publicação do edital;
- 6.75. Capacidades globais:**
- 6.75.1. Deve ter capacidade para operar com pelo menos 3 (três) segmentos de redes distintas fisicamente através de portas de rede, permitindo configurar WAN, LAN e DMZ, conforme a necessidade;
- 6.75.2. Possuir suporte a pelo menos 254 (duzentos e cinquenta e quatro) endereços IP em cada interface de rede;
- 6.75.3. Instalação e configuração de toda a solução *remota* com técnicos qualificados;
- 6.75.4. Possuir mecanismo anti-suicídio para a administração remota, evitando que o administrador perca o acesso ao software por uma configuração equivocada;
- 6.75.5. Permitir a conexão simultânea de vários administradores;
- 6.75.6. Deverá permitir backup das configurações local e remoto de forma automatizada;
- 6.75.7. Auditoria de todas as ações realizadas na interface web, logon/logout, visualizações, adições, edições e exclusões;



6.75.8. Possibilitar o acesso para interface de configuração e administração via web em português, com total capacidade sobre os recursos e funcionalidades existentes;

6.75.9. Garantia e atualizações periódicas do software durante a vigência do contrato de prestação de serviços;

6.75.10. Documentação técnica, incluindo manuais de configuração, instalação e operação de toda a solução proposta, todos em português;

6.75.11. Licença para cadastramento de **até 150 usuários.**

6.76. VPN (Rede Privada Virtual):

6.76.1. Deve permitir a criação de túneis VPN (*Virtual Private Network*) dos tipos: *Site-to-Site* (sob o protocolo SSL ou IPSEC) com capacidade para no mínimo 20 (vinte) túneis, *Client-to-site* (sob o protocolo PPTP MSCHAP v2) com capacidade para no mínimo 200 (duzentos) túneis;

6.76.2. Permitir a implementação de pelo menos 1.000 (mil) regras de filtro de pacotes, organizadas por grupos com descrição e possibilidade de ativar/inativar determinado grupo de regras;

6.76.3. Permitir a implementação de regras orientadas à objetos, tais como: grupo de serviços e grupos de hosts/redes;

6.76.4. Possibilitar regras específicas para pelo menos os protocolos GRE, TCP, UDP e ICMP.

6.77. Proxy cachê e filtro de conteúdo:

6.77.1. Suporte a uso de filtro de conteúdo por domínio, endereço IP, palavra-chave ou extensão de arquivo;

6.77.2. Gerenciamento de regras dos filtros de conteúdo por grupos de: *host*, *usuários* e *horários*;

6.77.3. Suporte a uso do *Proxy* transparente para o protocolo HTTP, de forma a dispensar a configuração dos browsers das máquinas clientes;

6.77.4. Possibilidade de visualizar relatório do conteúdo HTTP (navegação) que fora passado pelo *Proxy*, visualizando o usuário (se autenticado) e/ou host (se transparente);

6.77.5. Possibilidade de visualização de relatórios do conteúdo HTTP (navegação) por meses, dias e horários, bem como a listagem dos sites mais acessados, listagem dos maiores arquivos transferidos e números de bytes transferidos por *host*;

6.77.6. Possibilidade de visualização, em tempo real, de consumo de banda, por *host* ou sub-rede;

6.77.7. Possibilidade de ordenação da visualização em crescente/decrescente do consumo de banda, tempo real, por *host* ou grupo;

6.77.8. Autenticação Integrada com *Active Directory*, transparente com SSO (*Single SignOn*);

6.77.9. Capacidade de armazenar as atualizações do *Windows Update* e os principais antivírus do mercado, bem como demais softwares a serem informados durante a implementação e/ou durante a vigência do contrato, com o intuito de economizar banda para cada atualização das estações de trabalho.

6.78. Balanceamento de carga através de múltiplos links:

6.78.1. Suporte à criação de várias tabelas de roteamento, de acordo com cada link de comunicação disponível;

6.78.2. Possibilidade de balancear o tráfego para cada link disponível, de acordo com as regras de especificação: por origem, por destino e/ou serviço;

6.78.3. Capacidade de proporcionar alta disponibilidade de acesso à Internet e da rede através do balanceamento e da redundância de links dos equipamentos: asseguram a estabilidade na conexão em caso de perda de um dos links ou, ainda, que todos trabalhem para assegurar a continuidade de um determinado serviço.

6.79. Controle de banda e QoS:

6.79.1. Capacidade de otimizar e priorizar os tráfegos realmente importantes da instituição, como, por exemplo, a priorização de videoconferências;



6.79.2. Fornecer serviço de controle de banda e QoS (*Quality of Services*) que permita criar regras para definir a velocidade máxima para determinado tipo de tráfego, baseado na origem, destino ou serviço, bem como por grupos de *hosts*.

6.80. Monitoramento de rede e hosts:

6.80.1. Fornecer serviço de monitoramento de rede que apresente o tráfego entrante e saínte gerado pelos *hosts* da rede com a especificação do uso dos protocolos;

6.82.2. Fornecer serviço de monitoramento de *hosts* que verifica e armazena a disponibilidade de determinados *hosts* cadastrados, com relatório de informações detalhadas como: disponibilidade e latência.

7. DAS CONDIÇÕES DE MANUTENÇÃO E DO SUPORTE TÉCNICO:

7.1. O prazo de atendimento começa a ser contado a partir da hora do acionamento do chamado técnico, através de telefone ou e-mail;

7.2. Tabela de solução do chamado:

| Severidade | Descrição | Métrica | Tempo de solução de atendimento |
|-----------------------------|---|------------------------|------------------------------------|
| 1 - Urgente | Serviço parado no ambiente de produção, incluindo reposição de peça defeituosa. | Prazo: em horas úteis. | Em até 04 (quatro) horas. |
| 2 - Muito Importante | Erros ou problemas recorrentes que impactam o ambiente de produção. | Prazo: em horas úteis. | Em até 08 (oito) horas. |
| 3 - Importante | Problemas contornáveis. | Prazo: em horas úteis. | Em até 48 (quarenta e oito) horas. |
| 4 - Informação | Consulta técnica, dúvidas em geral, monitoramento, dentre outros. | Prazo: em horas úteis. | Em até 72 (setenta) horas. |

7.3. Devem ser feitas reuniões gerenciais, mensais ou a critério do CONTRATANTE, para avaliação e acompanhamento dos serviços de manutenção e suporte técnico;

7.4. Devem ser feitas reuniões técnicas, mensais ou a critério do CONTRATANTE, para planejamento e execução de serviços de manutenção e suporte técnico, com vistas à melhoria do ambiente instalado;

7.5. Em caso de substituição de equipamento defeituoso, o equipamento substituto deve ser igual ou superior, do mesmo fabricante, em características técnicas;

7.6. Manter central de suporte técnico, indicando o número de telefone desta ou endereço eletrônico para abertura de chamados;

7.7. A CONTRATADA deverá disponibilizar os seguintes canais de atendimento para a abertura de chamados:

7.7.1. Sistema de registro de chamados;



7.7.2. Telefone;

7.7.3. E-mail;

7.8. Cada chamado deverá conter, no mínimo, o registro das informações abaixo:

7.8.1. Número do chamado;

7.8.2. Técnico responsável pelo atendimento;

7.8.3. Dados do responsável pela abertura do chamado;

7.8.4. Descrição do problema;

7.8.5. Situação do chamado (aberto, em atendimento, encerrado, etc.);

7.8.6. Severidade (conforme tabela número x);

7.8.7. Data e hora de abertura;

7.8.8. Histórico do atendimento.

8. IMPLANTAÇÃO

8.1. A CONTRATADA será responsável pela instalação, configuração, atualização com patches do fabricante, integração e testes de todos os produtos fornecidos, inclusive no ambiente atual, de forma a garantir o total funcionamento e operabilidade no ambiente computacional da CONTRATANTE.

8.2. A CONTRATADA deverá executar todas as atividades (física e lógica) de migração dos serviços que se encontrem em operação, sem ônus para a CONTRATANTE.

9. RESULTADOS ESPERADOS

9.1. Assegurar o provimento de infraestrutura de TI segura e adequada para que a CMVSM continue operacional.

9.2. Contribuir para garantia de um nível adequado de disponibilidade, autenticidade e confiabilidade das informações produzidas e armazenadas em meios tecnológicos.

9.3. Oferecer maior agilidade e eficácia no tratamento de incidentes envolvendo endpoints (estações de trabalho notebooks) comprometidos.

9.4. Evitar, mitigar e conter a propagação de pragas digitais facilitando o tratamento destes incidentes (vírus, malwares, spywares, dentre outros) com a administração centralizada da solução de proteção.

9.5. Permitir o controle de acesso à rede por dispositivos computacionais, permitindo o gerenciamento destes dispositivos.

9.6. Gerar melhoria de qualidade do serviço de proteção de endpoints.

9.7. Aquisição de 170 licenças sendo possível adquirir mais caso necessário pelo mesmo valor das já adquiridas.

9.8. A solução antivírus deverá gerenciar de forma centralizadas os clientes instalados nas estações de trabalho, utilizando licença de software com função de antivírus, antispymware, firewall, proteção contra intrusos (HIPS).

9.10. Desinstalação completa de quaisquer soluções similares atualmente existentes nas estações de trabalho da CMVSM.

9.11. Em resumo os serviços devem ser entregues de modo a prover segurança na camada de usuário, mitigando riscos capazes de impactar a produtividade dos colaboradores da Câmara e degradar o desempenho dos sistemas e redes corporativas.

9.12. As soluções devem fazer parte do catálogo de produtos comercializados e não ter sido descontinuados.

9.13. A solução fornecida não deve estar relacionada em listas “endofsale” e “endofsupport” do site do fabricante; Todas as licenças referentes aos sistemas operacionais, bancos de dados e softwares componentes da solução adquirida, inclusive os que forem implantados em ambiente virtualizado,



devem estar em nome da CONTRATANTE, legalizado, não sendo admitidas versões “shareware” ou “trial”.

9.14. Deverão ser fornecidos todas as documentações e manuais técnicos completos necessários à instalação, configuração e operação da solução; A documentação e manuais técnicos deverão estar em Português. Deverão ser fornecidos materiais técnicos e manuais em formato digital que permita a importação para base de conhecimento online (Microsoft Word, PDF, HTML etc).

10. CENTRAL DE ATENDIMENTO

10.1. A Contratada deverá manter Central de Atendimento na Web para registro, acompanhamento, resolução de problemas e esclarecimento de dúvidas.

10.2. Cada atendimento deverá possuir um identificador único para facilitar o acompanhamento das soluções.

10.3. O acesso à Central de Atendimento disponível para atender as demandas da Câmara de Vereadores deverá estar disponível pelos canais: por ligação telefônica gratuita (0800), via Central na Web e por correio eletrônico (e-mail).

10.4. A Central de Atendimento na Web deverá possibilitar pelo menos as seguintes funcionalidades:

10.5. Abertura / Acompanhamento de Chamados, regrados pelo SLA contratado.

10.6. Documentações do Cliente (manuais procedimentos e outros arquivos de interesse do contrato).

10.7. Emissão / Reimpressão de faturas e pagamentos.

10.8. Impressão Notas Fiscais Emitidas.

11. DEMAIS CONDIÇÕES PARA PRESTAÇÃO DE SERVIÇOS

11.1. A liberação dos serviços deverá estar disponível em até 20 dias após a contratação.

11.2. Os serviços deverão estar disponíveis durante 24 horas do dia, nos 7 dias da semana.

11.3. Toda a solução que contemplam os serviços acima deverá incluir Hardware, Software, Serviços de instalação e suporte técnico durante as 24 (vinte e quatro) horas do dia nos 365 (trezentos e sessenta e cinco) dias do ano, de forma ininterrupta.

11.4. Todos os materiais, respectivos acessórios e cabeamentos fornecidos deverão ser novos, e em perfeitas condições para sua instalação e operação imediata.

11.5. Em caso de dano ou paralisação parcial ou total do equipamento por decorrência da sua operação normal, caberá à empresa contratada a manutenção ou sua substituição por outro appliance de mesmas características técnicas e também recuperação das configurações, sem quaisquer ônus adicional.

12. QUALIFICAÇÃO TÉCNICA

12.1. Apresentar, no mínimo, 01 (um) atestado de capacidade técnica, emitidos por órgão da administração pública ou por empresa privada, para os quais a proponente tenha fornecido mão de obra terceirizada semelhantes ao objeto desta licitação, devendo estar expressos nos atestados todas as características dos serviços prestados, como:

12.1.1. identificação da pessoa jurídica eminente;

12.1.2. nome e cargo do signatário;

12.1.3. endereço completo do eminente;

12.1.4. período de vigência do contrato;

12.1.5. objeto contratual;

12.1.6. quantitativos executados;

12.1.7. outras informações técnicas necessárias e suficientes para a avaliação das experiências referenciadas pela Comissão de Licitação.

13. VIGÊNCIA DA CONTRATAÇÃO



13.1. A vigência do contrato será de 12 meses, iniciando-se na data de assinatura do contrato, podendo ser prorrogado, se conveniente para a Administração, por iguais e sucessivos períodos, limitada a duração a 48 (quarenta e oito) meses, nos termos do art. 57, IV, da Lei Federal nº 8.666/93.

14. PAGAMENTO

14.1. O pagamento será efetuado em até 05 (cinco) dias úteis após liquidação da Nota Fiscal, que deverá estar devidamente visada pelo responsável pelo recebimento e conferência do objeto contratado.

14.2. Não haverá, sob qualquer hipótese, qualquer pagamento adiantado à efetiva entrega do objeto contratado.

14.3. Os pagamentos far-se-ão em moeda corrente nacional e serão creditados em nome do Contratado, após o efetivo cumprimento do objeto contratado devidamente atestado pela fiscalização, mediante ordem bancária em conta corrente indicada pela Empresa ou por meio de ordem bancária para o pagamento de Nota(s) Fiscal(is), Fatura(s) ou Documento de Cobrança de Valor Jurídico Equivalente, com “código de barras”, uma vez satisfeitas as condições estabelecidas neste Termo de Referência.

14.3.1. Serão descontadas do valor do pagamento as eventuais multas que lhe tenham sido impostas em decorrência de inadimplência contratual.

14.3.2. Qualquer erro ou omissão havido na documentação fiscal ou na fatura será objeto de correção pela empresa e haverá, em decorrência, suspensão do prazo de pagamento até que o problema seja definitivamente regularizado.

14.3.3. A Câmara de Vereadores reserva-se o direito de suspender o pagamento se o objeto for prestado em desacordo com as especificações constantes deste instrumento.

14.4. Tendo sido impostas penalidades ao CONTRATADO das quais não tenha recorrido tempestivamente, ou que já tenham sido objeto de decisão administrativa transitada em julgado, o respectivo valor será descontado do pagamento devido.

14.5. Todo e qualquer pagamento poderá ser sustado, se verificada qualquer das hipóteses a seguir elencadas e enquanto perdurar o ato/fato/omissão que a tiver motivado, sem direito a posterior reajuste, acréscimo, lucros cessantes, indenização, juros e/ou correção monetária:

14.5.1. retardar injustificadamente a execução do objeto da presente licitação;

14.5.2. haver infração à condição ou obrigação estabelecida no edital, contrato ou na proposta apresentada.

14.6. Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido, de alguma forma, para tanto, fica convencionado que a taxa de compensação financeira devida pela Contratante, entre a data do vencimento e o efetivo adimplemento da parcela, é calculada mediante a aplicação da seguinte fórmula:

$$EM = I \times N \times VP$$

14.6.1. Sendo:

EM = Encargos moratórios;

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = Valor da parcela a ser paga.

I = Índice de Compensação Financeira = 0,00016438



14.6.1.1. O Índice de Compensação Financeira (I) mencionado no subitem anterior é apurado da seguinte forma

$I = (TX = \text{Percentual da Taxa Anual} = 6\%)$

$I = (6 / 100) / 365$

$I = 0,00016438$

15. DA FISCALIZAÇÃO DO CONTRATO

15.1. O cumprimento das obrigações da CONTRATADA será acompanhado e fiscalizado pelo Fiscal de Contratos indicado pela CONTRATANTE, que anotará em registro próprio todas as ocorrências relacionadas com a execução dos serviços, determinando o que for necessário à regularização das falhas ou impropriedades observadas, nos termos dos arts. 67 e 73 da Lei Federal nº 8.666/1993.

15.2. Além do acompanhamento e da fiscalização da execução dos serviços, a CONTRATANTE poderá sustar qualquer serviço que esteja sendo executado em desacordo com o especificado, sempre que essa medida se tornar necessária.

15.3. À fiscalização compete encaminhar à Presidência da CONTRATANTE o documento que relacione as ocorrências que impliquem multas a serem aplicadas à CONTRATADA.

15.4. A ação da fiscalização não exonera a CONTRATADA de suas responsabilidades contratuais.

16. DA METODOLOGIA DE JULGAMENTO

16.1. O julgamento das propostas de preços será pelo critério de MENOR PREÇO GLOBAL, sendo declarada vencedora a Licitante que apresentar o menor preço e que atender a todos os requisitos e exigências contidas neste Termo de Referência.

17. DOS DIREITOS E OBRIGAÇÕES

17.1. Constituem direitos, da CONTRATANTE, receber o serviço contratado nas exatas condições avençadas e, da CONTRATADA, perceber o valor ajustado na forma e no prazo convencionados.

17.2. DAS OBRIGAÇÕES DA CONTRATANTE

17.2.1. Prestar as informações e os esclarecimentos que venham a ser solicitados pela CONTRATADA;

17.2.2. Efetuar o pagamento na forma e no prazo pactuados;

17.2.3. Rejeitar, no todo ou em parte, o objeto que a CONTRATADA entregar fora das especificações constantes neste Contrato.

17.3. DAS OBRIGAÇÕES DA CONTRATADA

17.3.1. Entregar o objeto contratado conforme convencionado, sem qualquer encargo ou despesa para o contratante fora das previsões contratuais;

17.3.2. Cumprir integralmente as obrigações assumidas, especialmente quanto aos prazos estabelecidos e às condições de entrega do objeto;

17.3.3. Utilizar produtos de excelente qualidade para a execução do serviço;

17.3.4. Assumir responsabilidade exclusiva por todos os ônus e tributos, emolumentos, honorários ou despesas incidentais sobre os serviços contratados, bem como cumprir rigorosamente e responsabilizar-se por todas as obrigações trabalhistas, previdenciárias e acidentárias relativas ao pessoal que empregar para a execução dos serviços, inclusive as decorrentes de convenções, acordos ou dissídios coletivos;



17.3.5. Realizar o reparo ou a correção, às suas expensas, dos serviços efetuados em desconformidade com o pactuado, que apresentem vícios, defeitos ou incorreções resultantes de sua execução;

17.3.6. Comunicar à CONTRATANTE qualquer alteração que possa comprometer a manutenção do contrato, nos casos estabelecidos no art. 65 da Lei 8.666/93;

17.3.7. Manter, durante toda a execução do contrato e em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas, de acordo com o previsto no art. 55, XIII da Lei Federal 8.666/93.

18. DAS PENALIDADES

18.1. Pelo descumprimento, parcial ou total, das condições previstas na proposta ou no contrato, a CONTRATANTE poderá aplicar à CONTRATADA as seguintes sanções previstas no art. 87, da Lei 8.666/93, sem prejuízo da responsabilização civil e penal cabíveis:

18.1.1. Advertência formal, por intermédio do setor competente, quando ocorrer descumprimento de cláusulas contratuais que não justifiquem a aplicação de penalidade mais grave;

18.1.2. Multa de Mora equivalente a 0,5 % (meio por cento) sobre o valor global do contrato, para cada dia de atraso no início da prestação do serviço.

18.1.2.1. A multa de que trata o item anterior não impedirá a rescisão unilateral do contrato pela CONTRATANTE, na forma dos artigos 77 e seguintes da Lei 8.666/1993;

18.1.3. Multa sobre o valor total atualizado no contrato:

18.1.3.1. De até 2% (dois por cento) pelo descumprimento de cláusula contratual ou norma da legislação pertinente;

18.1.3.2. De até 30% (trinta por cento) nos casos de inexecução total ou parcial do contrato.

18.1.4. Suspensão do direito de licitar e contratar com a Administração, por período de até 24 (vinte e quatro) meses, de acordo com a natureza e a gravidade da falta, sem prejuízo da aplicação de multa, obedecida a seguinte graduação:

18.1.4.1. Após advertência formal e cobrança de multa, ser reincidente, sem justificativa, nas penalidades avençadas neste Contrato: Prazo da Suspensão de até 12 (doze) meses;

18.1.4.2. Não iniciar a execução da prestação do serviço no prazo estabelecido, desobedecendo à solicitação por escrito da CONTRATANTE: Prazo da Suspensão até 24 (vinte e quatro) meses.

18.1.5. Declaração de Inidoneidade para licitar e contratar com a Administração Pública, em função de falta de natureza grave, sem prejuízo de multas incidentes, publicada no Diário Oficial do Estado;

18.1.6. Outras penalidades previstas nas Leis Federais nº 8.666/1993 e 10.520/2002.

18.2. A aplicação de qualquer das penalidades previstas realizar-se-á mediante prévio e regular processo administrativo, que assegurará, absolutamente, o contraditório e a ampla defesa ao licitante/adjudicatário, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente na Lei nº 9.784, de 1999.

18.3. As penalidades previstas neste Termo de Referência poderão deixar de ser aplicadas, total ou parcialmente, a critério da CONTRATANTE, se entender como relevantes as justificativas apresentadas pela CONTRATADA.

18.3.1. Eventuais multas aplicadas deverão ser liquidadas simultaneamente com o pagamento da parcela vinculada ao evento cujo descumprimento deu origem à aplicação da penalidade;



18.3.2. Caso a multa não seja recolhida nas condições acima descritas, será descontada do pagamento da parcela vinculada ao evento cujo descumprimento deu origem à aplicação da penalidade.

19. DOS RECURSOS ORÇAMENTÁRIOS

19.1. Os recursos orçamentários desta contratação correrão por conta das seguintes dotações orçamentárias:

011220001.2.108 – Manutenção das Atividades Administrativas:
3.3.90.40.10.00.00 – Suporte a Usuários de T.I.C.

20. DO REAJUSTE E DO REEQUILÍBRIO ECONÔMICO-FINANCEIRO

20.1. Os preços do Contrato não sofrerão reajustes, conforme § 1º do art. 2º da Lei Federal nº 10.192, de 14 de fevereiro de 2001.

20.2. Os preços do Contrato poderão ser recompostos, em consonância com o que dispõe o artigo 65, inciso II, alínea “d”, da Lei Federal 8.666/1993.

21. DA SUBCONTRATAÇÃO, FUSÃO, CISÃO OU INCORPORAÇÃO

21.1. É vedada a subcontratação, total ou parcial, do objeto, a associação do contratado com outrem, a cessão ou transferência (total ou parcial), bem como a fusão, cisão ou incorporação, constituindo motivos para rescisão do contrato.

WALTER OPPERMANN
Diretor Administrativo da CMVSM



ANEXO III

MODELO DE DECLARAÇÃO DE ENQUADRAMENTO

() MICROEMPREENDEDOR INDIVIDUAL – MEI

() MICROEMPRESA – ME

() EMPRESA DE PEQUENO PORTE – EPP

A empresa _____ (RAZÃO SOCIAL DA EMPRESA), inscrita no CNPJ sob o nº _____, por intermédio de seu representante legal o(a) Sr.(a) _____, portador(a) da Carteira de Identidade nº _____, CPF nº _____, declara, para fins de obter os benefícios concedidos pela Lei Complementar nº 123/2006 e pela Lei Municipal nº 5.245/2009, que:

- Está enquadrada na condição de _____ (Microempreendedor Individual, Microempresa ou Empresa de Pequeno Porte) e que não incorre nas vedações a que se reporta o § 4 do art. 3º da Lei Complementar 123/2006;
- Apresenta à Receita Federal, anualmente, a Declaração de Informações Econômico-Fiscais da Pessoa Jurídica (DIPJ) e/ou Declaração Anual do Simples Nacional (DASM), em conformidade com o disposto em ato da Secretaria da Receita Federal;
- Conserva em boa ordem, pelo prazo de 05 (cinco anos), contados da data da emissão, os documentos que comprovam a origem das receitas e a efetivação das despesas, bem assim a realização de quaisquer outros atos ou operações que venham a modificar a situação patrimonial;
- Assume o compromisso de informar imediatamente ao Cadastro de Fornecedores - CRC da Secretaria Municipal de Finanças do Município de Santa Maria – RS qualquer alteração no porte da empresa que venha ocorrer no período de validade do Certificado emitido pelo CRC.

Está ciente de que a prestação de informações inverídicas sujeitará, juntamente com as demais pessoas que para ela concorrem, às penalidades previstas na legislação criminal e tributária relativas à falsidade ideológica (Art. 299 do Código Penal) e ao crime a ordem tributária (Art. 1º da Lei nº 8.137, de 27 de dezembro de 1990).

Esta Declaração não exime a responsabilidade da empresa em informar, a qualquer tempo, através de Declaração, alterações que tenha ocorrido em seu porte.

Local, ____ de _____ de 2019.

Nome e Assinatura do representante contábil (com CRC)

Observação: esta Declaração deverá estar datada dos últimos 180 dias anteriores à data da sessão de abertura dos Envelopes.



ANEXO IV
DO VALOR MÁXIMO UNITÁRIO E TOTAL ADMITIDOS POR ITEM
PREGÃO PRESENCIAL Nº 07/2019

Objeto: Contratação de empresa capacitada para prestar serviço de solução para gerenciamento de conectividade de redes e prevenção de ameaças com suporte remoto para até 180 usuários.

| Item | Descrição | Quant. | Valor máximo unitário | Valor total |
|------|--|----------|-----------------------|-------------|
| 1 | Atualização anual das vacinas e software, caso necessário (a partir do segundo ano). | 170 | 147,50 | 25.075,00 |
| 2 | Solução de segurança para servidores (licença de uso para antivírus, somente no primeiro ano). | 3 | 182,50 | 547,50 |
| 3 | Aquisição de software para solução endpoint (licença de software, somente no primeiro ano). | 167 | 150,00 | 25.050,00 |
| 4 | Suporte técnico remoto (mensal e permanente durante a vigência do contrato – estimado em 120 horas para 12 meses). | 12 meses | 820,00 | 9.840,00 |
| 5 | Instalação e treinamento remoto inicial, a ser pago uma única vez, no primeiro ano somente. | 1 | 9.250,00 | 9.250,00 |
| 6 | Solução para gerenciamento de conectividade de redes (mensal e permanente durante a vigência do contrato). | 12 meses | 2.291,67 | 27.500,04 |

Valor total máximo admitido para o primeiro ano: R\$ 72.187,54 (setenta e dois mil cento e oitenta e sete reais e cinquenta e quatro centavos).

Valor total máximo admitido para o segundo ano: R\$ 62.415,04 (sessenta e dois mil quatrocentos e quinze reais e quatro centavos).



ANEXO V

PROPOSTA DE PREÇO - PREGÃO PRESENCIAL Nº 07/2019

Tipo: **MENOR PREÇO**
Aquisição: **GLOBAL**

Abertura: 02/07/2019.
Horário: 14:00 HORAS.

| |
|--------------|
| Empresa: |
| Endereço: |
| CNPJ: |
| Fone/e-mail: |

1. Apresentamos a Vossa Senhoria a nossa proposta de preço, detalhada na planilha abaixo, para a aquisição dos itens de que trata o **Pregão Presencial nº 07/2019**, conforme especificação constante do **Edital** e dos **Anexos**.

2. Declaramos que conhecemos e estamos de acordo com os termos do **Pregão Presencial nº 07/2019**. Se vencedora entregaremos os itens propostos pelos preços a seguir relacionados, já incluídos todos os impostos, custos e encargos diretos e indiretos, taxas, fretes, bem como deduzidos todos os descontos por nós concedidos:

| Item | Descrição | Quant. | Valor unitário | Valor total | Marca |
|------|--|----------|----------------|-------------|-------|
| 1 | Atualização anual das vacinas e software, caso necessário (a partir do segundo ano). | 170 | | | |
| 2 | Solução de segurança para servidores (licença de uso para antivírus, somente no primeiro ano). | 3 | | | |
| 3 | Aquisição de software para solução endpoint (licença de software, somente no primeiro ano). | 167 | | | |
| 4 | Suporte técnico remoto (mensal e permanente durante a vigência do contrato – estimado em 120 horas para 12 meses). | 12 meses | | | |
| 5 | Instalação e treinamento remoto inicial, a ser pago uma única vez, no primeiro ano somente. | 1 | | | |
| 6 | Solução para gerenciamento de conectividade de redes (mensal e permanente durante a vigência do contrato). | 12 meses | | | |

3. **Importante:** informar a marca na proposta, sob pena de desclassificação. Em caso de contratação, não serão aceitas marcas diferentes, por ocasião do recebimento.

Dados da Empresa:

- a) Razão Social: _____;
- b) CNPJ nº: _____;
- c) Inscrição Estadual nº: _____;
- d) Inscrição Municipal nº: _____;
- e) Endereço: _____;



Câmara Municipal de Vereadores de Santa Maria
Centro Democrático Adelman Simas Genro

- f) Fone: _____ Fax (se houver): _____;
g) E-mail: _____;
h) CEP: _____;
i) Cidade: _____; Estado: _____;
j) Responsável legal que assinará o contrato: _____;
k) Endereço do responsável legal que assinará o contrato: _____;
l) RG do responsável legal que assinará o contrato: _____;
m) CPF responsável legal que assinará o contrato: _____.

Local e data

Assinatura e Nome
(Representante Legal)

Observação: Emitir em papel timbrado.



ANEXO VI

PREGÃO PRESENCIAL Nº 07/2019

DECLARAÇÃO

(RAZÃO SOCIAL DA EMPRESA, inscrita no CNPJ nº _____, por intermédio
de seu representante legal o(a) Sr.(a)
_____, portador da Carteira de
Identidade nº _____, CPF nº _____, **DECLARA** que **não foi**
declarada inidônea e que **inexistem fatos impeditivos** para sua habilitação no presente Processo
Licitação, bem como ter ciência da obrigatoriedade de declarar ocorrências posteriores.

_____, de _____ de 2019.

Assinatura e Nome
(Representante Legal)

(Observação: em caso afirmativo, assinalar a ressalva acima)



ANEXO VII

PREGÃO PRESENCIAL Nº 07/2019

DECLARAÇÃO

_____, (RAZÃO SOCIAL DA EMPRESA), inscrito no CNPJ nº _____,
por _____ intermédio de seu representante legal o(a) Sr.(a) _____,
Identidade nº _____, CPF nº _____, portador da Carteira de
_____, **DECLARA** que para fins do
disposto no inciso V do art. 27 da Lei nº 8.666/93, de 21 de junho de 1993, acrescido pela Lei nº
9.854, de 27 de outubro de 1999, **não emprega menores** de dezoito anos em trabalho noturno,
perigoso ou insalubre, **e não emprega menor** de dezesseis anos.

Ressalva: emprega menor, a partir de quatorze anos, na condição de aprendiz (_____).

_____, de _____ de 2019.

Assinatura e Nome
(Representante Legal)

(Observação: em caso afirmativo, assinalar a ressalva acima)



ANEXO VIII

MODELO DE PROCURAÇÃO – PREGÃO PRESENCIAL Nº 07/2019

DECLARAÇÃO

NOME DA EMPRESA _____, CNPJ nº _____, por intermédio de seu representante legal o(a) Sr.(a) _____ portador da Carteira de Identidade nº _____, CPF nº _____, sediada _____ (Endereço Completo), **DECLARA**, sob as penas da lei, para fins do disposto no inciso VII da Lei nº 10.520, de 17 de julho de 2002, **que cumpre com os requisitos de habilitação previstos no edital do Pregão Presencial nº 07/2019.**

Local e Data

Assinatura e Nome
(Representante Legal)

(ESTA DECLARAÇÃO DEVERÁ SER APRESENTADA AO PREGOEIRO NO MOMENTO DO CREDENCIAMENTO).



ANEXO IX

MODELO DE PROCURAÇÃO – PREGÃO PRESENCIAL Nº 07/2019

PROCURAÇÃO

OUTORGANTE

Qualificação (nome, endereço e razão social, etc.)

OUTORGADO

Nome e qualificação

OBJETO

Representar o outorgante na Licitação, modalidade Pregão Presencial nº 07/2019.

PODERES

Apresentar documentação e propostas, participar de sessões públicas de abertura de documentos de habilitação e de propostas, assinar as respectivas atas, registrar ocorrências, formular impugnações, interpor recursos, renunciar ao direito de recurso e assinar todos os atos e quaisquer documentos indispensáveis ao bom e fiel cumprimento do presente mandato.

ASSINATURA DO(A) DIRETOR(A) OU SÓCIO(A)-GERENTE

Carimbo da empresa

(ESTA DECLARAÇÃO DEVERÁ SER APRESENTADA AO PREGOEIRO NO MOMENTO DO CREDENCIAMENTO).



ANEXO X

PORTARIA Nº 73/2019



Câmara Municipal de Vereadores
Centro Democrático Adelmo Simas Genro

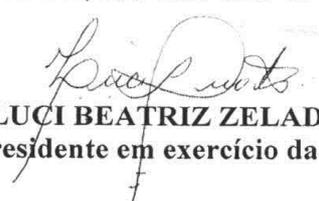
PORTARIA Nº. 073/2019

Designa pregoeiro e equipe de apoio para a realização de licitações na modalidade pregão no âmbito do Poder Legislativo Municipal de Santa Maria, para o ano de 2019.

Ver^a. LUCI BEATRIZ ZELADA DUARTES, Presidente em exercício da Câmara Municipal de Vereadores de Santa Maria, Estado do Rio Grande do Sul.

FAÇO SABER, na conformidade dos poderes que me são conferidos pela Legislação Vigente, que ficam designados os servidores **GIOVANI COSTA DE OLIVEIRA** como pregoeiro titular e **CRISTIANO PORTELA FOLLADOR** como pregoeiro suplente, para a realização de licitações na modalidade Pregão no âmbito do Poder Legislativo Municipal, para o ano de 2019. A equipe de apoio será composta pelos servidores **CRISTIANO PORTELA FOLLADOR, LEONIR DUTRA SOBRINHO, MARLI PREVEDELLO VIEIRA, MARCELO SALDANHA MACHADO (1º SUPLENTE) e ELIANE ELISABETE DOS SANTOS SOARES (2º SUPLENTE)** a partir de 11/01/2019.

Gabinete da Presidência da Câmara Municipal de Vereadores de Santa Maria, Estado do Rio Grande do Sul, aos onze dias do mês de janeiro do ano de dois mil e dezenove.


Ver^a. LUCI BEATRIZ ZELADA DUARTES
Presidente em exercício da CMVSM

**Registre-se e
Cumpra-se.**

Ver. ALEXANDRE VARGAS
1º. Secretário


Arnaldo Vanderlei Ochulaki – Alemão do Gás
Vereador – PSB

Rua Vale Machado, 1415 – Santa Maria – RS Cep: 97010-530
Home Page: www.camara-sm.rs.gov.br
Email: cmvsm@camara-sm.rs.gov.br
Telefone: (055) 3220 7200