**PREGÃO ELETRÔNICO Nº 18/2018**

**AMPLA CONCORRÊNCIA**

|  |  |  |
| --- | --- | --- |
| PROCESSO | : | TC/011017/2019 |
| MODALIDADE | : | Pregão ELETRÔNICO |
| **OBJETO** | **:** | **Aquisição de Solução, em Alta Disponibilidade, de FIREWALL UTM/NGFW do tipo Appliance, com Fonte Redundante e Cluster, incluindo Hardware, Software, Banco de Horas, Vouchers de Treinamento, Serviços de Instalação, Configuração e Suporte Técnico 24x7.** |
| TIPO | : | Menor preço |
| LOCAL DA SESSÃO PÚBLICA | : | Portal de Compras do Governo Federal – <http://www.comprasnet.gov.br> |
| DATA DE ABERTURA | : | **20 de setembro de 2019** |
| HORÁRIO | : | **09h00** |

O ***TRIBUNAL DE CONTAS DO MUNICÍPIO DE SÃO PAULO,*** com sede na Avenida Professor Ascendino Reis nº 1130, Vila Clementino, nesta Capital, torna público para conhecimento de quantos possam interessar que, em obediência ao que preceituam os Decretos Municipais nº 44.279, de 24 de dezembro de 2003, nº 46.662, de 24 de novembro de 2005, Lei Municipal nº 13.278 de 2002, Lei Federal nº 8.666/93 e alterações posteriores, Lei Federal nº 10.520/02, Leis Complementares nº 123/06, 147/14 e 155/16, dos Decretos Municipais nº 43.406, de 08 de julho de 2003, nº 47.014, de 21 de fevereiro de 2006, nº 54.102, de 17 de julho de 2013, com alterações inseridas pelo Decreto Municipal nº 54.829, de 10 de fevereiro de 2014, Decreto nº 56.475, de 05 de outubro de 2015 e demais normas pertinentes, fará realizar licitação na modalidade **PREGÃO ELETRÔNICO**, a ser processada pela Comissão Permanente de Licitação nº 2 do Tribunal, atuando seu Presidente como Pregoeiro. Este certame terá como critério de julgamento o **MENOR PREÇO,** em conformidade com as disposições deste Edital e respectivos Anexos.

1. DO OBJETO
	1. O objeto da presente licitação é a escolha da proposta mais vantajosa para a **aquisição de solução, em alta disponibilidade, de *FIREWALL UTM/NGFW* do tipo *appliance*, com fonte redundante e *cluster*, incluindo *hardware, software*, banco de horas, *vouchers* de treinamento, serviços de instalação, configuração e suporte técnico 24x7,** conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.
2. DOS RECURSOS ORÇAMENTÁRIOS
	1. As despesas resultantes do presente instrumento correrão por conta dos recursos constantes das dotações orçamentárias 77.10.01.032.3014.2818.4490.52 – Equipamentos e Material Permanente e 10.10.01.032.3024.2818.3390.40 – Serviços de Tecnologia da Informação e Comunicação – Pessoa Jurídica.
3. DO CREDENCIAMENTO
	1. O Credenciamento é o nível básico do registro cadastral no Sistema de Cadastramento Unificado de Fornecedores – SICAF, que permite a participação dos interessados na modalidade licitatória Pregão, em sua forma eletrônica e dar-se-á pela atribuição, pelo órgão provedor, de chave de identificação e de senha, pessoal e intransferível, para acesso ao sistema eletrônico**.**
	2. O cadastro no SICAF poderá ser iniciado no Portal de Compras do Governo Federal, no sítio www.comprasgovernamentais.gov.br, com a solicitação de *login* e senha pelo interessado.
	3. O credenciamento junto ao provedor do sistema implica a responsabilidade do licitante ou de seu representante legal e a presunção de sua capacidade técnica para realização das transações inerentes a este Pregão.
	4. O uso da senha de acesso pelo licitante é de sua responsabilidade exclusiva, incluindo qualquer transação efetuada diretamente ou por seu representante, não cabendo ao provedor do sistema, ou ao Tribunal de Contas do Município de São Paulo, promotor da licitação, responsabilidade por eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros.
	5. A perda da senha ou a quebra de sigilo deverão ser comunicadas imediatamente ao provedor do sistema para imediato bloqueio de acesso.
	6. Nenhuma pessoa, ainda que munida de procuração, poderá representar mais de uma empresa no presente certame, sob pena de exclusão sumária das representadas.
4. DA PARTICIPAÇÃO NO PREGÃO
	1. Poderão participar deste Pregão interessados cujo ramo de atividade seja compatível com o objeto desta licitação, e que estejam com Credenciamento regular no Sistema de Cadastramento Unificado de Fornecedores – SICAF, nos termos do Decreto 3.722/2001, com a redação conferida pelo Decreto nº 4.485/2002.
		1. As empresas não cadastradas no SICAF que tiverem interesse em participar do presente PREGÃO deverão providenciar o seu cadastramento e sua habilitação junto a qualquer unidade cadastradora dos Órgãos da Administração Pública.
	2. Não poderão participar desta licitação os interessados:
		1. Declarados inidôneos para licitar e contratar com a Administração Pública;
		2. Proibidos de participar de licitações e celebrar contratos administrativos, na forma da legislação vigente;
			1. De acordo com a Resolução do TCMSP nº 08, de 29 de setembro de 2016, a sanção prevista no inciso III do art. 87 da Lei Federal nº 8.666/1993, tal como as previstas no inciso IV, do mesmo artigo, e no art. 7º da Lei Federal nº 10.520/2002, projeta efeitos para todos os órgãos e entidades de todos os entes federativos.
		3. Estrangeiros que não tenham representação legal no Brasil com poderes expressos para receber citação e responder administrativa ou judicialmente;
		4. Que se enquadrem nas vedações previstas no art. 9º da Lei nº 8.666/93;
		5. Cuja falência tenha sido decretada; e
		6. Entidades empresariais que estejam reunidas em consórcio.
	3. Como condição para participação no Pregão, o licitante assinalará “sim” ou “não” em campo próprio do sistema eletrônico, relativo às seguintes declarações:
		1. Que cumpre os requisitos estabelecidos no artigo 3° da Lei Complementar nº 123/2006, estando apto a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49.
			1. A assinalação do campo “não” apenas produzirá o efeito de o licitante não ter direito ao tratamento favorecido previsto na Lei Complementar nº 123, de 2006, mesmo que microempresa ou empresa de pequeno porte, **quando esta não for condição para sua participação no certame**;
			2. A falsidade das declarações prestadas, objetivando os benefícios da Lei Complementar nº 123/2006, poderá caracterizar o crime de que trata o art. 299 do Código Penal, sem prejuízo do enquadramento em outras figuras penais e das sanções administrativas previstas na legislação pertinente, mediante o devido processo legal, e implicará, também, o afastamento do licitante, se o fato vier a ser constatado durante o trâmite da licitação.
		2. Que está ciente e concorda com as condições contidas no Edital e seus anexos, bem como de que cumpre plenamente os requisitos de habilitação definidos no Edital;
		3. Que inexistem fatos impeditivos para sua habilitação no certame, ciente da obrigatoriedade de declarar ocorrências posteriores;
		4. Que não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do art. 7°, inciso XXXIII, da Constituição Federal.
		5. Que a proposta foi elaborada de forma independente.
5. DO ENVIO DA PROPOSTA
	1. O licitante deverá encaminhar a(s) proposta(s) por meio do sistema eletrônico até a data e horário marcados para abertura da sessão, quando, então, encerrar-se-á automaticamente a fase de recebimento de propostas.
	2. Todas as referências de tempo no Edital, no aviso e durante a sessão pública observarão o horário de Brasília – DF.
	3. O licitante será responsável por todas as transações que forem efetuadas em seu nome no sistema eletrônico, assumindo como firmes e verdadeiras suas propostas e lances.
	4. Incumbirá ao licitante acompanhar as operações no sistema eletrônico durante a sessão pública do Pregão, ficando responsável pelo ônus decorrente da perda de negócios diante da inobservância de quaisquer mensagens emitidas pelo sistema, de sua desconexão ou por sua omissão quando chamado à manifestação via “chat”.
	5. Até a abertura da sessão, os licitantes poderão retirar ou substituir as propostas apresentadas.
	6. O licitante deverá enviar sua proposta mediante o preenchimento, no sistema eletrônico, dos seguintes campos:
		1. **Preço** correspondente ao **valor total de cada item**, de acordo com os preços praticados no mercado, conforme estabelece o art. 43, inciso IV, da Lei nº 8.666/1993, em algarismo, expresso em moeda corrente nacional (R$), considerando as quantidades constantes do Anexo I deste Edital.
		2. Descrição detalhada do objeto, conforme especificações previstas no Termo de Referência.
	7. Todas as especificações do objeto contidas na proposta vinculam a Contratada.
	8. Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente sobre o objeto a ser contratado por este Edital.
		1. A Contratada deverá arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, tais como os valores providos com o quantitativo de vale transporte, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da licitação, exceto quando ocorrer algum dos eventos arrolados nos incisos do §1° do artigo 57 da Lei n° 8.666, de 1993.
		2. Caso o eventual equívoco no dimensionamento dos quantitativos se revele superior às necessidades da contratante, a Administração deverá efetuar o pagamento seguindo estritamente as regras contratuais de faturamento dos serviços demandados e executados, concomitantemente com a realização, se necessário e cabível, de adequação contratual do quantitativo necessário, com base na alínea "b" do inciso I do art. 65 da Lei n. 8.666/93.
	9. O prazo de validade da proposta não será inferior a 60 (sessenta) dias**,** a contar da data de sua apresentação.
6. DA FORMULAÇÃO DE LANCES
	1. A abertura da presente licitação dar-se-á em sessão pública, por meio de sistema eletrônico, na data, horário e local indicados neste Edital.
	2. O Pregoeiro verificará as propostas apresentadas, desclassificando desde logo aquelas que não estejam em conformidade com os requisitos estabelecidos neste Edital, contenham vícios insanáveis, ilegalidades, ou apresentarem irregularidades ou defeitos capazes de dificultar o julgamento.
		1. A desclassificação será sempre fundamentada e registrada no sistema, com acompanhamento em tempo real por todos os participantes.
		2. A não desclassificação da proposta não impede o seu julgamento definitivo em sentido contrário, levado a efeito na fase de aceitação.
	3. O sistema ordenará automaticamente as propostas classificadas, sendo que somente estas participarão da fase de lances.
	4. Iniciada a etapa competitiva, os licitantes poderão oferecer lances sucessivos, exclusivamente por meio do sistema eletrônico, sendo o licitante imediatamente informado do seu recebimento e respectivos horário de registro e valor.
		1. O lance deverá ser ofertado pelo **valor total do item.**
	5. Não haverá intervalo mínimo de diferença de valores entre os lances.
	6. O licitante somente poderá oferecer lance inferior ao último por ele ofertado e registrado pelo sistema.
		1. O intervalo entre os lances enviados pelo mesmo licitante não poderá ser inferior a vinte (20) segundos e o intervalo entre lances não poderá ser inferior a três (3) segundos
	7. Não serão aceitos dois ou mais lances de mesmo valor, prevalecendo aquele que for recebido e registrado em primeiro lugar.
	8. Durante o transcurso da sessão pública, os licitantes serão informados, em tempo real, do valor do menor lance registrado, vedada a identificação do licitante.
	9. No caso de desconexão com o Pregoeiro, no decorrer da etapa competitiva do Pregão, o sistema eletrônico poderá permanecer acessível aos licitantes para a recepção dos lances.
	10. Se a desconexão perdurar por tempo superior a 30 (trinta) minutos, a sessão poderá ser suspensa, tendo reinício somente após comunicação expressa do Pregoeiro aos participantes.
	11. O critério de julgamento adotado será o **menor preço total**, conforme definido neste Edital e seus anexos.
	12. A etapa de lances da sessão pública será encerrada por decisão do Pregoeiro. O sistema eletrônico encaminhará aviso de fechamento iminente dos lances, após o que transcorrerá período de tempo de até 30 (trinta) minutos, aleatoriamente determinado pelo sistema, findo o qual será automaticamente encerrada a recepção de lances.
	13. Caso o licitante não apresente lances, concorrerá com o valor de sua proposta e, na hipótese de desistência de apresentar outros lances, valerá o último lance por ele ofertado, para efeito de ordenação das propostas.
	14. Encerrada a etapa de lances, será efetivada a verificação automática, junto à Receita Federal, do porte da entidade empresarial. O sistema identificará em coluna própria as microempresas e empresas de pequeno porte, procedendo**, nos casos em que a licitação permita a ampla participação**, à comparação com os valores da primeira colocada, se esta for empresa de maior porte, assim como das demais classificadas, para o fim de aplicar-se o disposto nos arts. 44 e 45 da LC nº 123, de 2006, regulamentada pelo Decreto Municipal nº 56.475, de 05 de outubro de 2015.
		1. Nessas condições, as propostas de microempresas e empresas de pequeno porte que se encontrarem na faixa de até 5% (cinco por cento) acima da proposta ou lance de menor preço serão consideradas empatadas com a primeira colocada.
		2. A melhor classificada nos termos do item anterior terá o direito de encaminhar uma última oferta para desempate, obrigatoriamente em valor inferior ao da primeira colocada, no prazo de 5 (cinco) minutos controlados pelo sistema, contados após a comunicação automática para tanto.
		3. Caso a microempresa ou a empresa de pequeno porte melhor classificada desista ou não se manifeste no prazo estabelecido, serão convocadas as demais licitantes microempresa e empresa de pequeno porte que se encontrem naquele intervalo de 5% (cinco por cento), na ordem de classificação, para o exercício do mesmo direito, no prazo estabelecido no subitem anterior.
		4. Só se aplica o sorteio quando houver empate entre as propostas e ausência de lances. Lances equivalentes não serão considerados iguais, vez que a ordem de apresentação pelos licitantes é utilizada como um dos critérios de classificação.
7. DO JULGAMENTO DAS PROPOSTAS
	1. Encerrada a etapa de lances, o Pregoeiro verificará o eventual descumprimento das condições de participação do licitante detentor da proposta classificada em primeiro lugar, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:
		1. SICAF;
		2. Cadastro Nacional de Empresas Inidôneas e Suspensas – CEIS, mantido pela Controladoria-Geral da União;
		3. Cadastro Nacional de Condenações Cíveis por Atos de Improbidade Administrativa, mantido pelo Conselho Nacional de Justiça;
		4. Lista de Inidôneos, mantida pelo Tribunal de Contas da União – TCU;
		5. Relação de empresas apenadas pelo Governo do Estado de São Paulo;
		6. Relação de empresas apenadas pela Prefeitura de São Paulo.
	2. A consulta aos cadastros será realizada em nome da empresa licitante e também de seu sócio majoritário, por força do art. 12 da Lei n° 8.429/1992, que prevê, dentre as sanções impostas ao responsável pela prática de ato de improbidade administrativa, a proibição de contratar com o Poder Público, inclusive por intermédio de pessoa jurídica da qual seja sócio majoritário.
	3. Constatada a existência de sanção, o Pregoeiro reputará o licitante inabilitado, por falta de condição de participação.
	4. Inexistindo qualquer impedimento o Pregoeiro examinará a proposta classificada em primeiro lugar quanto ao preço, a sua exequibilidade, bem como quanto ao cumprimento das especificações do objeto.
	5. Será desclassificada a proposta ou o lance vencedor que:
		1. Contenha vício insanável ou ilegalidade;
		2. Não apresente as especificações técnicas exigidas pelo Termo de Referência;
		3. Apresentar preço final superior ao preço máximo fixado, ou que apresentar preço manifestamente inexequível.
			1. Considera-se inexequível a proposta de preços ou menor lance que:
				1. Comprovadamente, for insuficiente para a cobertura dos custos da contratação, apresente preços global ou unitários simbólicos, irrisórios ou de valor zero, incompatíveis com os preços dos insumos e salários de mercado, acrescidos dos respectivos encargos, exceto quando se referirem a materiais e instalações de propriedade do próprio licitante, para os quais ele renuncie a parcela ou à totalidade da remuneração.
			2. Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderão ser efetuadas diligências, na forma do § 3° do art. 43 da Lei n° 8.666/1993.
	6. O Pregoeiro poderá encaminhar, por meio do sistema eletrônico, contraproposta ao licitante que apresentou o lance mais vantajoso, com o fim de negociar a obtenção de melhor preço, vedada a negociação em condições diversas das previstas neste Edital.
		1. Também nas hipóteses em que o Pregoeiro não aceitar a proposta e passar à subsequente, poderá negociar com o licitante para que seja obtido preço melhor.
	7. A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais licitantes. Sempre que a proposta não for aceita, e antes de o Pregoeiro passar à subsequente, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos artigos 44 e 45 da LC nº 123, de 2006, seguindo-se a disciplina antes estabelecida, se for o caso e a licitação permitir a ampla participação.
8. **DO ENCAMINHAMENTO E ACEITABILIDADE DA PROPOSTA**
	1. O licitante detentor da melhor oferta, em prazo definido pelo pregoeiro, nunca inferior a 30 (trinta) minutos, contado da solicitação efetuada no sistema eletrônico, deverá encaminhar:
		1. A **proposta** final, conforme modelo do Anexo IV:
			1. Ser redigida em língua portuguesa, datilografada ou digitada, em uma via, sem emendas, rasuras, entrelinhas ou ressalvas, devendo a última folha ser assinada e as demais rubricadas pelo licitante ou seu representante legal.
			2. Indicar nome ou razão social da proponente, nº do CNPJ, endereço completo, telefone, e-mail, bem como o nome e nº do RG de seu representante legal;
			3. Ter validade não inferior a 60 (sessenta) dias, contados a partir da data de sua apresentação;
			4. Conter a indicação do banco, número da conta e agência do licitante detentor da melhor proposta, para fins de pagamento.
		2. **DECLARAÇÃO** de que os produtos fornecidos são novos, de primeiro uso e estão em linha de fabricação na data de abertura das propostas;
		3. **DECLARAÇÃO** de que a empresa fornecedora é parceira oficial e tem condições comercializar, instalar, configurar e prestar manutenção na solução ofertada.
			1. As comprovações poderão ser efetuadas por intermédio do sítio do fabricante (cópia da *home page* do fabricante no Brasil), ou por declaração da proponente, sob as penas da lei, de que faz parte do programa de parceria do fabricante da solução.
			2. Na hipótese de a proponente juntar a declaração prevista em 8.1.3.1 deverá, como condição para assinatura do contrato, juntar declaração, certificado ou contrato de distribuição emitido pelo fabricante, nos termos do item 13.4, “c” deste edital.
	2. O licitante deverá demonstrar, na forma da lei, que possui poderes para formular ofertas e lances de preços, bem como praticar todos os demais atos pertinentes ao certame.
	3. A proposta final deverá ser documentada nos autos, devendo ser observada no decorrer da execução do contrato e na aplicação de eventual sanção à Contratada, se for o caso.
		1. Todas as especificações do objeto contidas na proposta vinculam a Contratada.
	4. Qualquer interessado poderá requerer que se realizem diligências para aferir a exequibilidade e a legalidade das propostas, devendo apresentar as provas ou os indícios que fundamentam a suspeita.
	5. O Pregoeiro poderá convocar o licitante para enviar documento digital, por meio de funcionalidade disponível no sistema, estabelecendo no “chat” prazo mínimo de 20 (vinte) minutos, sob pena de não aceitação da proposta.
		1. O prazo estabelecido pelo Pregoeiro poderá ser prorrogado por solicitação escrita e justificada do licitante, formulada antes de findo o prazo estabelecido, e formalmente aceita pelo Pregoeiro.
	6. Se a proposta ou lance vencedor for desclassificado, o Pregoeiro examinará a proposta ou lance subsequente, e, assim sucessivamente, na ordem de classificação.
	7. Havendo necessidade, o Pregoeiro suspenderá a sessão, informando no “*chat*” a nova data e horário para a continuidade da mesma.
9. DA HABILITAÇÃO
	1. Os documentos exigidos para habilitação abaixo relacionados, deverão ser apresentados em meio digital pelos licitantes, por meio de funcionalidade presente no sistema (upload), no prazo de 02 (duas) horas após solicitação do Pregoeiro no sistema eletrônico.
		1. Somente mediante autorização do Pregoeiro e em caso de indisponibilidade do sistema, será aceito o envio da documentação por meio do e-mail claudio.barone@tcm.sp.gov.br.
	2. Posteriormente, os documentos de habilitação e proposta deverão ser remetidos em original, por qualquer processo de cópia reprográfica, autenticada por tabelião de notas, ou por servidor da Administração, desde que conferidos com o original, ou publicação em órgão da imprensa oficial, para análise, no prazo de 02 (dois) dias úteis, contados da aceitação da proposta” pelo Pregoeiro, à Comissão de Licitações que processou o certame, no seguinte endereço: Av. Professor Ascendino Reis, 1.130, Vila Clementino – São Paulo/SP, CEP 04027-000.
	3. Os licitantes deverão apresentar a documentação relativa à Habilitação Jurídica, Regularidade Fiscal e trabalhista, Qualificação Econômico-Financeira e Qualificação Técnica conforme discriminado nos tópicos seguintes:
	4. **Habilitação jurídica:**
		1. No caso de empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;
		2. Em se tratando de microempreendedor individual – MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio www.portaldoempreendedor.gov.br;
		3. No caso de sociedade empresária ou empresa individual de responsabilidade limitada - EIRELI: ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado na Junta Comercial da respectiva sede, acompanhado de documento comprobatório de seus administradores;
		4. Em se tratando de sociedades comerciais ou empresa individual de responsabilidade limitada: ato constitutivo em vigor, devidamente registrado, e, no caso de sociedades por ações, acompanhado de documentos de eleição de seus administradores;
		5. Inscrição no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz, no caso de ser o participante sucursal, filial ou agência;
		6. Inscrição do ato constitutivo no Registro Civil das Pessoas Jurídicas, no caso de sociedades simples, acompanhada de prova de diretoria em exercício;
		7. Decreto de autorização, em se tratando de sociedade empresária estrangeira em funcionamento no País;
		8. Os documentos acima deverão estar acompanhados de todas as alterações ou da consolidação respectiva;
	5. **Regularidade fiscal e trabalhista:**
		1. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas (CNPJ);
		2. Prova de inscrição no cadastro de contribuintes estadual ou municipal, se houver, relativo ao domicílio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;
		3. Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02/10/2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.
		4. Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);
		5. Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943 (Certidão Negativa de Débitos Trabalhistas);
		6. Certidão Negativa de débitos referentes a tributos estaduais relacionados com o objeto licitado, do domicílio ou sede do licitante.
			1. Os licitantes com domicílio ou sede no Estado de São Paulo deverão comprovar a regularidade fiscal por meio da Certidão Negativa de Débitos Tributários da Dívida Ativa do Estado de São Paulo, expedida pela Procuradoria Geral do Estado, conforme Portaria CAT nº 20, de 1º de abril de 1998.
		7. Prova de regularidade com a Fazenda Municipal do domicílio ou sede do licitante, relativamente aos tributos mobiliários;
			1. Caso o licitante seja considerado isento dos tributos municipais relacionados ao objeto licitatório, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda Municipal do seu domicílio ou sede, ou outra equivalente, na forma da lei;
			2. Caso o licitante não esteja cadastrado como contribuinte neste Município, deverá apresentar também declaração firmada pelo seu representante legal/procurador, sob as penas da lei, do não cadastramento e de que nada deve à Fazenda do Município de São Paulo, relativamente aos tributos mobiliários, conforme modelo constante do Anexo II.
		8. O licitante detentor da melhor proposta, enquadrado como microempresa ou empresa de pequeno porte, deverá apresentar toda a documentação exigida para efeito de comprovação de regularidade fiscal, mesmo que esta apresente alguma restrição, sob pena de inabilitação.
		9. Serão aceitas como prova de regularidade certidões positivas com efeito de negativas que noticiem em seu corpo que os débitos estão judicialmente garantidos ou com sua exigibilidade suspensa.
	6. **Qualificação técnica:**
		1. Operacional
			1. **ATESTADO(S) DE CAPACIDADE TÉCNICA ou CERTIDÃO (ÕES)**, emitido(s) por pessoa jurídica de direito público ou privado, em nome da empresa licitante, devidamente datado(s), assinado(s) e com a identificação do atestante, que comprove(m) que o licitante tenha cumprido perfeitamente as obrigações relativas à prestação de serviços semelhantes ao objeto desta licitação.
				1. O(s) atestado(s) ou certidão(ões) deverá(ão) ser apresentado(s) em papel timbrado, assinado por autoridade ou representante de quem o expediu, com a devida identificação, devendo conter o nome, o endereço e o telefone de contato do(s) atestador(es), **comprovando o fornecimento de bens e prestação de serviços compatíveis com o objeto da licitação.**

Poderá ser utilizado mais de um atestado para comprovar a qualificação técnica solicitada.

Poderá ser realizada diligência para comprovar a autenticidade do atestado de capacidade técnica.

* 1. **Qualificação Econômico-Financeira:**
		1. Certidão negativa de falência ou recuperação judicial expedida pelo distribuidor do principal estabelecimento da pessoa jurídica, em data não superior a 60 (sessenta) dias da data da abertura do certame, se outro prazo não constar do documento.
			1. No caso de certidão positiva, o licitante deverá juntar a Certidão de Objeto e Pé, expedida pelo órgão competente, esclarecendo o posicionamento da(s) ação(ões).
			2. No caso de sociedade simples, a proponente deverá apresentar certidão dos processos cíveis em andamento relativos à solvência ou não do licitante, expedido pelo distribuidor da sede de pessoa jurídica, em data não superior a 60 (sessenta) dias da data da abertura do certame, se outro prazo não constar do documento.
	2. As empresas, cadastradas ou não no SICAF, deverão apresentar ainda:
		1. DECLARAÇÃO subscrita por quem detenha poderes de representação, sob as penas do art. 299 do Código Penal, se for o caso, de que se enquadra na situação de microempresa, empresa de pequeno porte ou cooperativas, nos termos da Lei Complementar nº 123/2006 e do Decreto nº 56.475/2015, bem como de que inexistem fatos supervenientes que conduzam ao seu desenquadramento dessa situação conforme modelo constante do Anexo III.
			1. No caso de microempreendedor individual, a declaração poderá ser substituída pelo Certificado de Condição de Microempreendedor Individual – CCMEI, emitido pelo Portal do Empreendedor.
		2. Não serão aceitos documentos com indicação de CNPJ/CPF diferentes, salvo aqueles legalmente permitidos.
	3. A comprovação da regularidade fiscal e trabalhista, da qualificação econômico-financeira e da habilitação jurídica, conforme o caso, poderá ser substituída pela consulta ao SICAF, nos casos em que a empresa estiver habilitada no referido sistema, conforme o disposto nos arts. 4º, caput, 8º, § 3º, 13 a 18 e 43, III, da Instrução Normativa SLTI/MPDG nº 2, de 11 de outubro de 2010.
		1. Também poderão ser consultados os sítios oficiais emissores de certidões, especialmente quando o licitante esteja com alguma documentação vencida junto ao SICAF.
		2. Caso o Pregoeiro não logre êxito em obter a certidão correspondente através do sítio oficial, ou na hipótese de se encontrar vencida no referido sistema, o licitante será convocado a encaminhar, no prazo de 02 (duas) horas, documento válido que comprove o atendimento das exigências deste Edital, sob pena de inabilitação.
	4. A existência de restrição relativamente à regularidade fiscal e trabalhista, conforme estatui o art. 43, § 1º da Lei Complementar nº 123/2006, não impede que o licitante qualificado como microempresa ou empresa de pequeno porte seja declarado vencedor, uma vez que atenda a todas as demais exigências do edital.
		1. A declaração do vencedor acontecerá no momento imediatamente posterior à fase de habilitação.
		2. Os licitantes, ainda que pretendam apresentar sua regularidade fiscal ou trabalhista com alguma restrição, nos termos da Lei Complementar nº 123/2006, deverão declarar o cumprimento dos requisitos de habilitação, uma vez que neste Edital constam as exigências próprias para quem pretender se utilizar deste benefício, ficando, portanto, implícita a ressalva da possibilidade de apresentação de documentação afeta à regularidade fiscal com restrição e regularização “a posteriori”.
	5. Uma vez constatada a existência de alguma restrição no que tange à regularidade fiscal ou trabalhista o licitante será convocado para, no prazo de 5 (cinco) dias úteis após a declaração do vencedor, nos termos da Lei Complementar nº 123/2006, comprovar a regularização. O prazo poderá ser prorrogado por igual período, a critério da administração pública, quando requerida pelo licitante, mediante apresentação de justificativa.
		1. A não-regularização fiscal no prazo previsto no subitem anterior acarretará a inabilitação do licitante, sem prejuízo das sanções previstas neste Edital, com a reabertura da sessão pública.
	6. Havendo necessidade de analisar minuciosamente os documentos exigidos, o Pregoeiro suspenderá a sessão, informando no “chat” a nova data e horário para a continuidade da mesma.
	7. Será inabilitado o licitante que não comprovar sua habilitação, seja por não apresentar quaisquer dos documentos exigidos, ou apresentá-los em desacordo com o estabelecido neste Edital.
	8. No caso de inabilitação seguir-se-á a disciplina antes estabelecida para aceitação da proposta subsequente.
	9. Todos os documentos deverão estar em nome da licitante e, preferencialmente com o número do CNPJ, e endereço respectivo.
		1. Se a licitante for a matriz, todos os documentos deverão estar em nome da matriz;
		2. Se a licitante for a filial, todos os documentos deverão estar em nome da filial, exceto aqueles que pela própria natureza, forem comprovadamente emitidos apenas em nome da matriz;
		3. Se a licitante for a matriz e a fornecedora for a filial, os documentos deverão ser apresentados em nome da matriz e da filial simultaneamente.
	10. Os documentos apresentados deverão estar com seu prazo de validade em vigor. Se este prazo não constar de cláusula específica do Edital, do próprio documento ou de lei aplicável à espécie, será considerado o prazo de validade de 06 (seis) meses, a contar de sua expedição.
	11. Da sessão pública do Pregão divulgar-se-á Ata no sistema eletrônico.
1. DA REABERTURA DA SESSÃO PÚBLICA
	1. A sessão pública poderá ser reaberta:
		1. Nas hipóteses de provimento de recurso que leve à anulação de atos anteriores à realização da sessão pública precedente ou em que seja anulada a própria sessão pública, situação em que serão repetidos os atos anulados e os que dele dependam.
		2. Quando houver erro na aceitação do preço melhor classificado ou quando o licitante declarado vencedor não assinar o contrato, não retirar o instrumento equivalente ou não comprovar a regularização fiscal, nos termos do art. 43, §1º da Lei Complementar nº 123/2006. Nessas hipóteses, serão adotados os procedimentos imediatamente posteriores ao encerramento da etapa de lances.
	2. Todos os licitantes remanescentes deverão ser convocados para acompanhar a sessão reaberta.
		1. A convocação se dará por meio do sistema eletrônico (“chat”) ou e-mail, de acordo com a fase do procedimento licitatório.
		2. A convocação feita por e-mail dar-se-á de acordo com os dados contidos no SICAF, sendo responsabilidade do licitante manter seus dados cadastrais atualizados.
2. DOS RECURSOS
	1. O Pregoeiro declarará o vencedor e, depois de decorrida a fase de regularização fiscal de microempresa ou empresa de pequeno porte, se for o caso, concederá o prazo de no mínimo trinta minutos, para que qualquer licitante manifeste a intenção de recorrer, de forma motivada, isto é, indicando contra qual(is) decisão(ões) pretende recorrer e por quais motivos, em campo próprio do sistema.
	2. Havendo quem se manifeste, caberá ao Pregoeiro verificar a tempestividade e a existência de motivação da intenção de recorrer, para decidir se admite ou não o recurso, fundamentadamente.
		1. Nesse momento o Pregoeiro não adentrará no mérito recursal, mas apenas verificará as condições de admissibilidade do recurso.
		2. A falta de manifestação motivada do licitante quanto à intenção de recorrer importará a decadência desse direito.
		3. Uma vez admitido o recurso, o recorrente terá, a partir de então, o prazo de 03 (três) dias corridos para apresentar as razões, pelo sistema eletrônico, ficando os demais licitantes, desde logo, intimados para, querendo, apresentarem contrarrazões também pelo sistema eletrônico, em outros 03 (três) dias corridos, que começarão a contar do término do prazo do recorrente, sendo-lhes assegurada vista imediata dos elementos indispensáveis à defesa de seus interesses.
	3. O acolhimento do recurso invalida tão somente os atos insuscetíveis de aproveitamento.
	4. Os autos do processo permanecerão com vista franqueada aos interessados, no endereço constante neste Edital.
3. **DA ADJUDICAÇÃO E HOMOLOGAÇÃO**
	1. O objeto da licitação será adjudicado ao licitante declarado vencedor, por ato do Pregoeiro, caso não haja interposição de recurso, ou pela autoridade competente, após a regular decisão dos recursos apresentados.
	2. Após a fase recursal, constatada a regularidade dos atos praticados e mantida a conveniência da contratação, a autoridade competente homologará o procedimento licitatório.
4. **DAS CONDIÇÕES DE CONTRATAÇÃO E DO AJUSTE**
	1. As obrigações decorrentes desta licitação consubstanciar-se-ão nos termos da minuta de Contrato - Anexo V.
	2. A adjudicatária será convocada pelo Tribunal para, no prazo de 10 (dez) dias úteis, a contar da data de convocação, para assinar o Termo de Contrato.
	3. Antes de emitir o Termo de Contrato o Tribunal de Contas do Município de São Paulo efetuará consulta ao Cadastro Informativo Municipal (CADIN), conforme estabelecido no inciso I, art. 3º, da Lei nº 14.094/2005, ou na Legislação que vier a substituí-la.
		1. Caso exista registro de débito no CADIN, a Proponente adjudicatária estará impossibilitada de contratar com a Administração, salvo se estiver suspenso o impedimento, conforme dispositivo legal vigente, ou se a Proponente comprovar ter ajuizado ação com garantia oferecida, na forma da lei, ou ainda, comprovar estar suspensa a exigibilidade do crédito.
	4. Antes da assinatura do contrato, o licitante vencedor deverá apresentar, além dos documentos que estiverem vencidos:
		* 1. O **contrato social** e a **procuração** de plenos poderes para a sua assinatura;
			2. Os **certificados técnicos**, emitidos pelo fabricante, que comprovem que os técnicos são habilitados e capacitados para execução dos serviços de instalação e configuração dos respectivos itens.
			3. **Declaração, certificado ou contrato de distribuição** emitido pelo fabricante dos produtos, comprovando que a empresa proponente faz parte do seu programa de parceria.
	5. O prazo para a assinatura do contrato poderá ser prorrogado uma vez, desde que solicitado por escrito, antes do término do prazo, sob alegação de motivo justo que poderá ou não ser aceito pela Administração.
	6. Na hipótese do não atendimento à convocação ou havendo recusa em fazê-lo, a Administração convocará os demais licitantes, observada a ordem de classificação, independentemente das penalidades previstas neste Edital.
		1. Em caso de convocação das licitantes classificadas remanescentes, deverão ser averiguadas as condições de habilitação destas.
5. DAS OBRIGAÇÕES DA CONTRATANTE E DA CONTRATADA
	1. As obrigações da Contratante e da Contratada são as estabelecidas no Termo de Referência e no Termo de Contrato.
6. DO PREÇO E DO PAGAMENTO
	1. Conforme previsto na Minuta de Contrato - Anexo V.
7. DAS SANÇÕES ADMINISTRATIVAS.
	1. Comete infração administrativa, nos termos da Lei nº 10.520/2002, o licitante/adjudicatário que:
		1. Não assinar o termo de contrato ou aceitar/retirar o instrumento equivalente, quando convocado dentro do prazo de validade da proposta;
		2. Apresentar documentação falsa;
		3. Deixar de entregar os documentos exigidos no certame;
		4. Ensejar o retardamento da execução do objeto;
		5. Não mantiver a proposta;
		6. Cometer fraude fiscal;
		7. Comportar-se de modo inidôneo;
		8. Cometer falha ou fraude na execução das obrigações assumidas
	2. Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os licitantes, em qualquer momento da licitação, mesmo após o encerramento da fase de lances.
	3. O licitante/adjudicatário que cometer qualquer das infrações discriminadas nos subitens anteriores ficará sujeito, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:
		1. Multa de 15% (quinze por cento) sobre o valor estimado do(s) item(s) prejudicado(s) pela conduta do licitante;
		2. Impedimento de licitar e de contratar, bem como o descredenciamento no SICAF, pelo prazo de até 05 (cinco) anos;
	4. A penalidade de multa pode ser aplicada cumulativamente com a sanção de impedimento.
	5. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa ao licitante/adjudicatário, observando-se o procedimento previsto na Lei nº 8.666/1993, e subsidiariamente na Lei nº 14.141, de 27 de março de 2006 (Lei de Processo Administrativo do Município de São Paulo).
	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 o procedimento previsto no Capítulo X do Decreto Municipal nº 44.279/03 e na Seção II do Capítulo 4 da Lei Federal nº 8.666/93.
	7. As importâncias relativas às multas serão descontadas, sempre que possível, do pagamento a que tiver direito a CONTRATADA, ou cobradas judicialmente, se for o caso.
	8. As sanções por atos praticados no decorrer da contratação estão previstas no Termo de Referência.
8. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO
	1. Até 02 (dois) dias úteis antes da data designada para a abertura da sessão pública, qualquer pessoa poderá impugnar este Edital.
	2. A impugnação poderá ser realizada por forma eletrônica, pelo e-mail **claudio.barone@tcm.sp.gov.br** ou por petição dirigida ou protocolada nos dias úteis, das 7h às 17h30 na Unidade Técnica de Protocolo e Autuação do TCMSP, na Av. Professor Ascendino Reis, 1.130, Vila Clementino – São Paulo/SP.
	3. Caberá ao Pregoeiro decidir sobre a impugnação no prazo de até vinte e quatro horas antes do horário previsto para a abertura do certame.
	4. Quando o acolhimento da impugnação implicar alteração do Edital, capaz de afetar a formulação das propostas, será designada nova data para a realização do certame.
	5. Os pedidos de esclarecimentos referentes a este processo licitatório deverão ser enviados ao Pregoeiro, até 03 (três) dias úteis anteriores à data designada para abertura da sessão pública, exclusivamente por meio eletrônico via internet, no endereço indicado no Edital.
	6. As impugnações e pedidos de esclarecimentos não suspendem os prazos previstos no certame.
	7. As respostas às impugnações e os esclarecimentos prestados pelo Pregoeiro serão entranhados nos autos do processo licitatório e estarão disponíveis para consulta por qualquer interessado.
9. DAS DISPOSIÇÕES GERAIS
	1. Fica o licitante ciente de que a apresentação da proposta implica a aceitação de todas as condições deste Edital e de seus anexos, não podendo invocar desconhecimento dos termos do instrumento convocatório ou das disposições legais aplicáveis à espécie para furtar-se ao cumprimento de suas obrigações.
	2. Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a realização do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subsequente, no mesmo horário anteriormente estabelecido, desde que não haja comunicação em contrário, pelo Pregoeiro, por meio de publicação no Diário Oficial da Cidade de São Paulo, pelo site www.tcm.sp.gov.br>Editais e no endereço eletrônico http://e-negocioscidadesp.prefeitura.sp.gov.br – Tribunal de Contas do Município de São Paulo.
	3. No julgamento das propostas e da habilitação, o Pregoeiro poderá sanar erros ou falhas que não alterem a substância das propostas, dos documentos e sua validade jurídica, mediante despacho fundamentado, registrado em ata e acessível a todos, atribuindo-lhes validade e eficácia para fins de habilitação e classificação.
	4. 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 documento ou informação que deveria constar no ato da sessão pública.
	5. O Presidente do TCMSP somente poderá revogar a licitação por razões de interesse público decorrente de fato superveniente devidamente comprovado, pertinente e suficiente para justificar tal conduta, devendo anulá-la por ilegalidade, de ofício ou por provocação de terceiros, mediante parecer escrito e devidamente fundamentado.
	6. A homologação do resultado desta licitação não implicará direito à contratação.
	7. As normas disciplinadoras da licitação serão sempre interpretadas em favor da ampliação da disputa entre os interessados, desde que não comprometam o interesse da Administração, o princípio da isonomia, a finalidade e a segurança da contratação.
	8. Os licitantes assumem todos os custos de preparação e apresentação de suas propostas e o TCMSP não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do processo licitatório.
	9. Na contagem dos prazos estabelecidos neste Edital e seus Anexos, excluir-se-á o dia do início e incluir-se-á o do vencimento. Só se iniciam e vencem os prazos em dias de expediente no TCMSP.
	10. O desatendimento de exigências formais não essenciais não importará o afastamento do licitante, desde que seja possível o aproveitamento do ato, observados os princípios da isonomia e do interesse público.
	11. Em caso de divergência entre disposições deste Edital e de seus anexos ou demais peças que compõem o processo, prevalecerá as deste Edital.
	12. Os casos omissos e as dúvidas surgidas serão resolvidos pelo Pregoeiro.
	13. O Edital está disponibilizado, na íntegra, no endereço eletrônico <http://www.tcm.sp.gov.br> - Editais e no endereço eletrônico http://e-negocioscidadesp.prefeitura.sp.gov.br – Tribunal de Contas do Município de São Paulo; e também poderão ser obtidos, mediante o pagamento correspondente ao custo da cópia reprográfica a ser recolhido aos cofres públicos, através de guia de recolhimento, das 9h às 17h, até o último dia que anteceder a data designada para a abertura do certame, na Av. Professor Ascendino Reis, 1.130, Vila Clementino – São Paulo/SP, com qualquer membro da Comissão de Licitações.
10. **DOS ANEXOS**
	1. Integram este Edital, para todos os fins e efeitos, os seguintes anexos:
		1. Anexo I - Termo de Referência
		2. Anexo II - Modelo de declaração sobre tributos municipais (**enviar com os documentos de Habilitação – subitem 9.5.7.2 do Edital**).
		3. Anexo III - Modelo de declaração de ME/EPP/Cooperativa e inexistência de fatos supervenientes (**subitem 9.8.1 do Edital**).
		4. Anexo IV - Modelo de proposta **(subitem 8.1.1 do Edital).**
		5. Anexo V - Minuta de Contrato.

São Paulo,

CLÁUDIO VICENTE PALADINO BARONE

Pregoeiro

**ANEXO I**

**TERMO DE REFERÊNCIA**

**I - OBJETO**

Aquisição de Solução, em Alta Disponibilidade, de FIREWALL UTM/NGFW do tipo *Appliance*, com Fonte Redundante e *Cluster*, incluindo *Hardware*, *Software*, Banco de Horas, *Vouchers* de Treinamento, Serviços de Instalação, Configuração e Suporte Técnico 24x7.

**II - PRODUTO**

|  |
| --- |
| **SOLUÇÃO** |
| **Item** | **Qtde.** | **Descrição** | **Garantia** |
| 01 | 01 | FIREWALL UTM/NGFW do tipo *Appliance*, com Fonte Redundante, *Cluster*, Licenças, Solução Virtual de Relatórios, Instalação, Configuração e Suporte Técnico 24x7 | 36 meses |
| **BANCO DE HORAS** |
| **Item** | **Qtde.** | **Descrição** | **Período** |
| 02 | 70 horas | Suporte nos dias úteis entre 9h e 18h | 36 meses |
| 03 | 80 horas | Suporte nos demais horários | 36 meses |
| **TREINAMENTO** |
| **Item** | **Qtde.** | **Descrição** | **Validade** |
| 04 | 02 Servidores | *Vouchers* | 12 meses |

**III – SOLUÇÃO DE SEGURANÇA DE REDE**

A Solução deverá ser composta por 02 (dois) equipamentos trabalhando em Alta Disponibilidade, contendo em cada um:

A*ppliance* com no máximo 2U de altura, com kit de montagem em rack de 19”.

Não serão permitidas soluções baseadas em sistemas operacionais abertos como Free BSD, Debian, ou mesmo Linux.

Cada equipamento deverá ser baseado em hardware desenvolvido com esta finalidade, ou seja, de um Firewall não sendo baseado em plataforma X86 ou equivalente.

A solução deverá utilizar a tecnologia de Firewall *Stateful Packet Inspection* com *Deep Packet Inspection* (suportar a inspeção da área de dados do pacote) para filtragem de tráfego IP.

Sistema Operacional do Tipo “Harderizado” não serão aceitos. Apenas os que forem armazenados em memória flash.

02 (duas) Fontes redundante de alimentação interna com operação automática entre 110/220V. Possuir redundância do sistema de refrigeração do produto (ventoinha).

Deverá ser capaz de suportar, no mínimo, 16 (dezesseis) interfaces Gbe (Gigabit ethernet) RJ45 e, no mínimo, 16 Slots SFP e distintas para console de gerência e Alta disponibilidade (HA), 2USB ports, todas integradas no equipamento.

O Gerenciamento Unificado de Ameaças UTM (*Unified Threat Management)*, para proteção de informação perimetral e de rede interna que inclui *stateful firewall* com capacidade de controle de tráfego de dados por identificação de usuários, controle de aplicação, administração de largura de banda (QoS), VPN IPsec e SSL, IPS, prevenção contra ameaças de vírus, *malwares*, Filtro de URL e inspeção de tráfego criptografado, deverá ser fornecida em hardware específico.

O hardware e o software fornecidos não podem constar, no momento da apresentação da proposta, em listas de Final de venda (*end-of-sale), Final de suporte (end-of-support), Final de suporte de engenharia (end-of-engineering-support)* ou término de todos os suportes oferecidos, venda de peças ou fim do ciclo de vida determinado pelo fabricante (*end-of-life)*, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante.

**IV – CARACTERÍSTICAS ESPECÍFICAS DE DESEMPENHO E HARDWARE DA SOLUÇÃO DE FIREWALL**

Throughput de, no mínimo, 20 Gbps com a funcionalidade de Firewall habilitada para tráfego IPv4 e IPv6, independentemente do tamanho do pacote.

Suporte a, no mínimo, 4 M de conexões simultâneas.

Suporte a, no mínimo, 300.000 novas conexões por segundo.

Throughput de, no mínimo, 20 Gbps de VPN IPSec.

Estar licenciado para suportar, sem o uso de licença, 2.000 túneis de VPN IPSEC *Site-to-Site* simultâneos.

Estar licenciado para suportar sem o uso de licença, 50.000 túneis de clientes VPN IPSEC simultâneos.

Throughput de, no mínimo, 2,5 Gbps de VPN SSL.

Suporte a, no mínimo, 500 clientes de VPN SSL simultâneos. Suportar no mínimo 5 Gbps de throughput de IPS.

Suportar no mínimo 3 Gbps de throughput de Inspeção SSL. Suportar *Threat Protection Througput*, de pelo menos 3Gbps.

Permitir gerenciamento integrado no appliance de no mínimo 150 *Access Points*, ou seja, gerenciamento local.

Deverá prover suporte a Fast Roaming em autenticação com Captive Portal. Deve suportar configurações de Captive Portal por SSID.

A controladora wireless deve permitir criar um Captive Portal no *software switch* integrado para redes WIFI e redes cabeadas.

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

Possuir, no mínimo, 8G de RAM e 16G de armazenamento interno flash, exclusivo para logs.

**V – CARACTERÍSTICAS GERAIS PARA SOLUÇÃO DE FIREWALL**

A solução deve consistir em plataforma de proteção de rede baseada em appliance com funcionalidades de Next Generation Firewall (NGFW), e console de gerência e monitoração.

Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões.

As funcionalidades de proteção de rede que compõe a plataforma de segurança podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação.

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

Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19”, incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação.

O *software* deverá ser fornecido em sua versão mais atualizada.

O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta.

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

Os dispositivos de proteção de rede devem possuir suporte a 4094 VLAN *Tags* 802.1q.

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

Os dispositivos de proteção de rede devem possuir suporte a *Policy based routing* ou *policy based forwarding*.

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

Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay. Os dispositivos de proteção de rede devem possuir suporte a DHCP *Server*. Os dispositivos de proteção de rede devem suportar *sFlow*.

Os dispositivos de proteção de rede devem possuir suporte a Jumbo Frames.

Os dispositivos de proteção de rede devem suportar sub-interfaces *ethernet* logicas. Deve suportar NAT dinâmico (Many-to-1).

Deve suportar NAT dinâmico (*Many-to-Many*). Deve suportar NAT estático (1-to-1).

Deve suportar NAT estático (*Many-to-Many*). Deve suportar NAT estático bidirecional 1-to-1. Deve suportar Tradução de porta (PAT).

Deve suportar NAT de Origem. Deve suportar NAT de Destino.

Deve suportar NAT de Origem e NAT de Destino simultaneamente.

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

Deve suportar NAT64 e NAT46.

Deve implementar o protocolo ECMP.

Deve implementar balanceamento de *link* por *hash* do IP de origem.

Deve implementar balanceamento de *link* por *hash* do IP de origem e destino.

Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, quatro *links*.

Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais.

Deve permitir monitorar via SNMP falhas de hardware, uso de recursos por número elevado de sessões, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster, ataques e estatísticas de uso das interfaces de rede.

Enviar log para sistemas de monitoração externos, simultaneamente.

Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL.

Proteção anti-spoofing.

Implementar otimização do tráfego entre dois equipamentos.

Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2). Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3).

Suportar OSPF *graceful restart*.

Os dispositivos de proteção devem ter a capacidade de operar de forma simultânea em uma única instância de *Firewall*, mediante o uso de suas interfaces físicas nos seguintes modos: Modo *Sniffer* (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3).

Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede.

Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação.

Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como *default gateway* das redes protegidas.

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

Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em modo transparente.

Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em *layer* 3.

Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em *layer* 3 e com no mínimo 03 equipamentos no *cluster*.

A configuração em alta disponibilidade deve sincronizar: Sessões.

A configuração em alta disponibilidade deve sincronizar: Configurações, incluindo, mas não limitado às políticas de *Firewall*, NAT, QOS e objetos de rede.

A configuração em alta disponibilidade deve sincronizar: Associações de Segurança das VPNs. A configuração em alta disponibilidade deve sincronizar:Tabelas FIB.

O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link. Deve possuir suporte a criação de sistemas virtuais no mesmo appliance.

A utilização dos dispositivos em alta disponibilidade não deve impor limitações quanto à utilização de sistemas virtuais (contextos).

Deve permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados por equipes distintas.

O gerenciamento da solução deve suportar acesso via SSH e interface WEB (HTTPS), incluindo, mas não limitado a exportar configuração dos sistemas virtuais (contextos) por ambas interfaces.

Controle, inspeção e de-criptografia de SSL por política para tráfego de Entrada (*Inbound*) e Saída (*Outbound*), sendo que deve suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolação das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos).

As funcionalidades de controle de aplicações, VPN IPSec e SSL, QOS, SSL e SSH *Decryption* e protocolos de roteamento dinâmico devem operar em caráter permanente, o licenciamento do dispositivo de segurança não pode ter nenhuma relação com sua configuração de rede como, mas não limitado a, configuração de interfaces, endereços lógicos, etc , podendo ser utilizado por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante.

**VI – CONTROLE DE POLÍTICAS DE FIREWALL**

Deverá suportar controles por zona de segurança. Controles de políticas por porta e protocolo.

Controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações.

Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança. Controle de políticas por código de País (Por exemplo: BR, USA, UK, RUS).

Controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (*Inbound*) e Saída (*Outbound*).

Deve suportar *offload* de certificado em inspeção de conexões SSL de entrada (*Inbound*). Deve de-criptografar tráfego *Inbound* e *Outbound* em conexões negociadas com TLS 1.2. Controle de inspeção e de-criptografia de SSH por política.

Bloqueios dos seguintes tipos de arquivos: bat, cab, dll, exe, bin, zip, tar e mp3. *Traffic shaping* QoS baseado em Políticas (Prioridade, Garantia e Máximo).

QoS baseado em políticas para marcação de pacotes (*diffserv marking*), inclusive por aplicações.

Suporte a objetos e regras IPV6. Suporte a objetos e regras multicast.

Deve suportar no mínimo três tipos de negação de tráfego nas políticas de *Firewall*: *Drop* sem notificação do bloqueio ao usuário, *Drop* com notificação do bloqueio ao usuário, Drop com opção de envio de ICMP *Unreachable* para máquina de origem do tráfego, TCP-*Reset* para o *client*, TCP-*Rese*t para o *server* ou para os dois lados da conexão.

Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.

1. **– CONTROLE DE APLICAÇÕES**

Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo.

Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos.

Reconhecer pelo menos 1700 aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado à peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, *voip*, áudio, vídeo, *proxy*, mensageiros instantâneos, compartilhamento de arquivos, e-mail.

Reconhecer pelo menos as seguintes aplicações: *bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs*, etc.

Deve inspecionar o *payload* de pacote de dados com o objetivo de detectar através de expressões regulares assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo.

Deve detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a *Encrypted* *Bittorrent* e aplicações VOIP que utilizam criptografia proprietária.

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.

Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante.

Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado a *Yahoo Instant* *Messenger* usando HTTP. A decodificação de protocolo também deve identificar funcionalidades especificas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivo dentro do *Webex*.

Identificar o uso de táticas evasivas via comunicações criptografadas. Atualizar a base de assinaturas de aplicações automaticamente.

Limitar a banda (*download*/*upload*) usada por aplicações (*traffic shaping*), baseado no IP de origem, usuários e grupos do LDAP/AD.

Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários.

Deve ser possível adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras.

Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos.

Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas.

Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão.

A criação de assinaturas personalizadas deve permitir o uso de expressões regulares, contexto (sessões ou transações), usando posição no *payload* dos pacotes TCP e UDP e usando decoders de pelo menos os seguintes protocolos: HTTP, FTP, NBSS, DCE RPC, SMTP, Telnet, SSH, MS-SQL, IMAP, DNS, LDAP, RTSP e SSL.

O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações.

Deve alertar o usuário quando uma aplicação for bloqueada.

Deve possibilitar que o controle de portas seja aplicado para todas as aplicações.

Deve possibilitar a diferenciação de tráfegos *Peer2Peer* (*Bittorrent, emule, neonet*, etc.) possuindo granularidade de controle/políticas para os mesmos.

Deve possibilitar a diferenciação de tráfegos de *Instant* *Messaging* (*AIM, Hangouts, Facebook Chat*, etc) possuindo granularidade de controle/políticas para os mesmos.

Deve possibilitar a diferenciação e controle de partes das aplicações, como por exemplo, permitir o Hangouts chat e bloquear a chamada de vídeo.

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

Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como: Tecnologia utilizada nas aplicações (*Client*-*Server*, *Browse* *Based*, *Network* *Protocol*, etc), Nível de risco da aplicação, categoria da aplicação bem como as que usem técnicas evasivas, utilizadas por malwares como uso excessivo de banda, tunelamento de tráfego ou transferência de arquivos, etc.

Enviar log para sistemas de monitoração externos, simultâneos.

Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL.

1. **– PREVENÇÃO DE AMEAÇAS**

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

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

As funcionalidades de IPS, Antivírus e Anti*-Spyware* devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante.

Deve sincronizar as assinaturas de IPS, Antivírus, Anti-*Spyware* quando implementado em alta disponibilidade ativo/ativo e ativo/passivo.

Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS, Anti-*Spyware* e Antivirus: permitir, permitir e gerar *log*, bloquear, bloquear IP do atacante por um intervalo de tempo e enviar *tcp*-*reset*.

As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração.

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

Exceções por IP de origem ou de destino devem ser possíveis nas regras e assinatura a assinatura.

Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-*Spyware*, possibilitando a criação de diferentes politicas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens.

Deve permitir o bloqueio de vulnerabilidades. Deve permitir o bloqueio de exploits conhecidos.

Deve incluir proteção contra ataques de negação de serviços.

Deverá possuir o seguinte mecanismo de inspeção de IPS: Análise de padrões de estado de conexões.

Deverá possuir o seguinte mecanismo de inspeção de IPS: Análise de decodificação de protocolo.

Deverá possuir o seguinte mecanismo de inspeção de IPS: Análise para detecção de anomalias de protocolo.

Deverá possuir o seguinte mecanismo de inspeção de IPS: Análise heurística. Deverá possuir o seguinte mecanismo de inspeção de IPS: IP *Defragmentation*.

Deverá possuir o seguinte mecanismo de inspeção de IPS: Remontagem de pacotes de TCP. Deverá possuir o seguinte mecanismo de inspeção de IPS: Bloqueio de pacotes malformados. Ser imune e capaz de impedir ataques básicos como: *Syn flood, ICMP flood, UDP flood*, etc.

Detectar e bloquear a origem de portscans.

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

Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS. Possuir assinaturas para bloqueio de ataques de *buffer overflow*.

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

Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS e anti-*Spyware*, permitindo a criação de exceções com granularidade nas configurações.

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

Suportar bloqueio de arquivos por tipo. Identificar e bloquear comunicação com botnets.

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

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

Deve permitir que na captura de pacotes por assinaturas de IPS seja definido o número de pacotes a serem capturados ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos.

Deve possuir a função de proteção à resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas.

Os eventos devem identificar o país de onde partiu a ameaça.

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

Proteção contra *downloads* involuntários usando HTTP de arquivos executáveis e maliciosos.

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

1. **– FILTRO DE URL**

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

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

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

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

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

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

Possuir pelo menos 60 categorias de URLs.

Deve possuir a função de exclusão de URLs do bloqueio, por categoria. Permitir a customização de página de bloqueio.

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

1. **– IDENTIFICAÇÃO DE USUÁRIOS**

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

Deve possuir integração com *Microsoft Active Directory* para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários.

Deve possuir integração e suporte a *Microsoft Active Directory* para os seguintes sistemas operacionais: *Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 e Windows Server 2012 R2 e Windows Server 2016*.

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

Deve possuir integração com *Radius* para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários.

Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em Usuários e Grupos de usuários.

Deve permitir o controle, sem instalação de cliente de *software*, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no *Firewall* (*Captive* Portal).

Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes *Citrix* e *Microsoft Terminal Server*, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços.

Deve implementar a criação de grupos customizados de usuários no *Firewall*, baseado em atributos do LDAP/AD.

Permitir integração com tokens para autenticação dos usuários, incluindo, mas não limitado a acesso a internet e gerenciamento da solução.

Prover no mínimo um token nativamente, possibilitando autenticação de duplo fator.

1. ***– QOS E TRAFFIC SHAPING***

Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como *youtube, ustream*, etc.) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo *streaming*.

Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem. Suportar a criação de políticas de QoS e *Traffic Shaping* por endereço de destino. Suportar a criação de políticas de QoS e *Traffic Shaping* por usuário e grupo do LDAP/AD.

Suportar a criação de políticas de QoS e Traffic Shaping por aplicações, incluindo, mas não limitado a *Skype, Bittorrent, YouTube* e *Azureus*.

Suportar a criação de políticas de QoS e Traffic Shaping por porta. O QoS deve possibilitar a definição de classes por Banda Garantida. O QoS deve possibilitar a definição de classes por Banda Máxima.

O QoS deve possibilitar a definição de classes por Fila de Prioridade.

Suportar priorização em tempo real de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype.

Suportar marcação de pacotes *Diffserv*, inclusive por aplicação. Suportar modificação de valores DSCP para o Diffserv.

Suportar priorização de tráfego usando informação de *Type of Service*. Disponibilizar estatísticas em tempo real para classes de QoS ou *Traffic Shaping*.

Deve suportar QOS (traffic-shapping), em interface agregadas ou redundantes.

1. **– FILTRO DE DADOS**

Permitir a criação de filtros para arquivos e dados pré-definidos. Os arquivos devem ser identificados por extensão e assinaturas.

Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos i(MS Office, PDF, etc.) identificados sobre aplicações (HTTP, FTP, SMTP, etc.).

Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos.

Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos.

Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular.

1. **– GEO LOCALIZAÇÃO**

Suportar a criação de políticas por geo-localização, permitindo o trafego de determinado País/Países sejam bloqueados.

Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos.

Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas.

– VPN

Suportar VPN *Site-to-Site* e *Cliente-To-Site*. Suportar IPSec VPN.

Suportar SSL VPN.

A VPN IPSEc deve suportar 3DES.

A VPN IPSEc deve suportar Autenticação MD5 e SHA-1.

A VPN IPSEc deve suportar Diffie-Hellman *Group* 1, *Group* 2, *Group* 5 e *Group* 14.

A VPN IPSEc deve suportar Algoritmo *Internet Key* *Exchange* (IKEv1 e v2).

A VPN IPSEc deve suportar AES 128, 192 e 256 (*Advanced Encryption Standard*). A VPN IPSEc deve suportar Autenticação via certificado IKE PKI.

Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, *Check Point*, *Juniper*, Palo Alto *Networks*, *Fortinet*, *SonicWall*.

Suportar VPN em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPSec IPv6.

Deve permitir habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSEc a partir da interface gráfica da solução, facilitando o processo de *throubleshooting*.

A VPN SSL deve suportar o usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB.

As funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente.

Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies.

Atribuição de DNS nos clientes remotos de VPN.

Deve permitir criar políticas de controle de aplicações, IPS, Antivírus, Anti-*Spyware* e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL.

Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local. Suportar leitura e verificação de CRL (certificate revocation list).

Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL.

O agente de VPN a ser instalado nos equipamentos *desktop* e *laptops*, deve ser capaz de ser distribuído de maneira automática via *Microsoft* SCCM, *Active* *Directory* e ser descarregado diretamente desde o seu próprio portal, o qual residirá no centralizador de VPN.

Deve permitir que a conexão com a VPN seja estabelecida da seguinte forma: Antes do usuário autenticar na estação.

Deve permitir que a conexão com a VPN seja estabelecida da seguinte forma: Após autenticação do usuário na estação.

Deve permitir que a conexão com a VPN seja estabelecida da seguinte forma: Sob demanda do usuário.

Deverá manter uma conexão segura com o portal durante a sessão.

O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows

*XP (32 bit), Windows 7 (32 e 64 bit), Windows 8 (32 e 64 bit), Windows 10 (32 e 64 bit) e Mac OS X (v10.10 ou superior*).

1. **– RELATÓRIOS**

Funcionalidades Gerais.

Possuir capacidade de receber ao menos 3 GBytes de logs diários. Possuir ao menos 1,5 TB de espaço em disco.

Suportar 10.000 devices/VDOMs.

Deve suportar Hypervision - VMware ESX/ESXi 5.0/5.1/5.5/6.0/6.5/6.7, Microsoft Hyper-V 2008 R2/2012/2012 R2/2016, Citrix XenServer 6.0+ and Open Source Xen 4.1+, KVM on Redhat 6.5+ and Ubuntu 17.04, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP), Oracle Cloud Infrastructure (OCI).

Deve possuir no mínimo 2 VCPUs.

Possuir ao menos 04 interfaces de suporte. Deve suportar pelo menos 4GB de memória.

1. **– REQUISITOS MÍNIMOS DE FUNCIONALIDADE**

Deve suportar acesso via SSH, WEB (HTTPS) e Telnet para o gerenciamento da solução.

Possuir comunicação cifrada e autenticada com usuário e senha para solução de relatórios, tanto como para a interface gráfica de usuário e console de administração por linha de comandos (SSH).

Permitir acesso simultâneo de administradores permitindo a criação de ao menos 02 perfis para administração e monitoração.

Suportar SNMP versão 2 e versão 3 na solução de relatórios.

Permitir virtualizar a solução de relatórios, onde cada administrador gerencie, visualize e edite apenas os dispositivos autorizados e cadastrados no seu ambiente virtualizado.

Deve permitir a criação de administradores que acessem a todas as instâncias de virtualização da solução de relatórios.

Deve permitir habilitar e desabilitar, para cada interface de rede da solução de relatórios, permissões de acesso HTTP, HTTPS, SSH, SNMP e *Telnet*.

Autenticação integrada a servidor Radius.

Geração de relatórios em tempo real, para a visualização de tráfego observado, nos formatos: mapas geográficos e tabela.

Geração de relatórios em tempo real, para a visualização de tráfego observado, no formato bolhas.

Autenticação integrada ao *Microsoft Active Directory*.

Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações.

Deve possuir um assistente para adicionar dispositivos via interface gráfica usando o IP, login e senha do mesmo.

Deve ser possível visualizar a quantidade de logs enviado de cada dispositivo monitorado. Possuir mecanismo para que logs antigos sejam removidos automaticamente.

Permitir a importação e exportação de relatórios.

Deve possuir a capacidade de criar relatórios nos formatos HTML. Deve possuir a capacidade de criar relatórios nos formatos PDF. Deve possuir a capacidade de criar relatórios nos formatos XML. Deve possuir a capacidade de criar relatórios nos formatos CSV. Deve ser possível exportar os logs em CSV.

Geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração.

Os logs gerados pelos appliances devem ser centralizados nos servidores de gerência, mas a solução deve oferecer também a possibilidade de utilização de um syslog externo ou similar.

A solução deve possuir relatórios pré-definidos.

Possuir envio automático de logs para um servidor FTP externo a solução. Possibilitar a duplicação de relatórios existentes e edita-los logo após.

Possuir a capacidade de personalização de capas para os relatórios.

Permitir de forma centralizada visualizar os logs recebidos por um ou vários dispositivos externos incluindo a capacidade de uso de filtros nas pesquisas deste *log*.

Logs de auditoria para configurações de regras e objetos devem ser visualizados em uma lista diferente da que exibe os logs relacionados a tráfego de dados.

Possuir a capacidade de personalização de gráficos como barra, linha e tabela para inserção aos relatórios.

Deve possuir mecanismo "*Drill*-*Down*" para navegação nos relatórios em *realtime*. Dever ser possível fazer download dos arquivos de logs recebidos.

Deve possuir agendamento para gerar e enviar automaticamente relatórios.

Permitir customização de quaisquer relatórios fornecidos pela solução, exclusivamente pelo administrador, adaptando-o às suas necessidades.

Permitir o envio de maneira automática de relatórios por *e*-*mail*.

Deve permitir a escolha do e-mail a ser enviado para cada relatório escolhido.

Permitir programar a geração de relatórios, conforme calendário definido pelo administrador.

Deve ser possível visualizar através de gráficos em tempo real o consumo de disco e taxa de geração de logs dos dispositivos gerenciados.

Deve ser possível definir filtros nos relatórios.

Deve ser capaz de definir o layout do relatório, incluir gráficos, inserir textos e imagens, alinhamento, quebras de páginas, definir fontes, cores, entre outros.

Permitir que relatórios criados sejam no idioma Português.

Gerar alertas automáticos via *e-mail*, SNMP e *Syslog* baseados em eventos como ocorrência como log, severidade de log, entre outros.

Deve permitir o envio automático de relatórios criado a um servidor de SFTP ou FTP externo a solução.

Deve ser capaz de criar consultas SQL ou semelhante para uso nos gráficos e tabelas de relatórios.

Ter a capacidade de visualizar na GUI da solução de relatórios informações do sistema como licenças, memória, disco, uso de CPU, taxa de logs por segundo recebidos, total de logs diários recebidos, alertas gerados entre outros.

Deve possuir uma ferramenta para análise de desempenho para cada relatório gerado, com o objetivo de detectar problemas de performance de sistema de acordo com o relatório criado.

Permitir que a solução importe arquivos de log, de dispositivos compatíveis conhecidos e não conhecidos pelo sistema, para posterior geração de relatórios.

Deve ser possível definir o espaço que cada instância de virtualização poderá utilizar para armazenamento de logs.

A solução deve servir como um servidor de syslog e aceitar logs de diferentes fabricantes.

Deve possuir a informação da quantidade de logs armazenado e estatística de tempo de retenção restante.

Deve suportar duplo fator de autenticação (*token*) para os administradores do sistema de relatórios.

Deve permitir aplicar políticas de senhas para os administradores do sistema como tamanho mínimo e caracteres a usar.

Deve permitir ver em tempo real os logs recebidos.

1. **– FUNCIONALIDADE DE RELATORIA**

Deve permitir a criação de *Dashboards* customizados para visibilidades do tráfego de aplicativos, categorias de URL, ameaças, serviços, países, origem e destino.

Deve possuir um Indicador de Comprometimento (IoC), que mostre usuários finais com utilização web suspeita, devendo informar no mínimo: endereço ip do usuário, hostname, sistema operacional, veredito (classificação geral de ameaça), número de ameaças detectadas.

Deve possuir relatório de PCI DSS Compliance.

Deve possuir relatório de utilização de aplicações SAAS.

Deve possuir relatório detalhado de prevenção de perda de dados (DLP). Deve possuir relatório de VPN.

Deve possuir relatório de Sistemas de prevenção de intrusão (IPS). Deve possuir relatório de reputação do cliente.

Deve possuir relatório de análise de segurança do usuário. Deve possuir relatório de avaliação da ameaça cibernética. Deve possuir relatório de *WiFi* PCI *Compliance*.

Deve possuir relatório a informação de AP´s e SSID´s autorizados, também clientes *WiFi*. Deve possuir relatório de equipamentos terminais de solução de segurança gerenciada. Deve possuir relatório de análise de segura.

1. **– SERVIÇOS DE INSTALAÇÃO E ENTREGA**

Os equipamentos deverão ser entregues embalados, sendo novo e de primeiro uso, não contendo nenhum tipo de violação na embalagem e com garantia do fabricante com o prazo mínimo de 36 meses.

A embalagem só poderá ser aberta pela CONTRATADA e na sede do CONTRATANTE no momento da instalação, como garantia de que o lacre não foi rompido ou adulterado durante o transporte.

Junto aos equipamentos deverão ser entregues os *softwares*, itens de acessórios de hardware incluindo (mas não se limitando a) cabos, conectores, *interfaces*, suportes, *drivers* de controle e programas de configuração, conforme especificações constantes neste Termo de Referência, necessários para o perfeito funcionamento da solução.

A reunião inicial para elaboração de cronograma com prazos, datas e responsáveis pelas atividades deverá ocorrer em até 05 dias corridos após a entrega dos Equipamentos e *Softwares*.

A entrega do material gerado dessa reunião deverá ser entregue em até 10 dias corridos, para validação pelos técnicos do TCMSP.

A instalação da solução deverá ocorrer em até 05 dias corridos, após a validação.

A CONTRATADA deverá elaborar o plano de testes, em conjunto com os técnicos do TCMSP, em até 10 dias após a instalação da solução.

Designar e apresentar um gerente técnico para representar a CONTRATADA perante o CONTRATANTE em questões de ordem técnica.

Elaborar cronograma do Plano de Implantação, contemplando as atividades que necessitem ser realizadas em dias úteis e não úteis, (instalação, configuração e integração da solução) incluindo, no mínimo, as seguintes fases do projeto: Planejamento, Instalação, Configuração, Testes e Validação funcional. Os serviços que prejudiquem o funcionamento normal das atividades do CONTRATANTE deverão ser realizados fora do horário comercial, estabelecido de comum acordo entre as partes.

Indicar recursos a serem alocados, e as pessoas que serão envolvidas no projeto como um todo. Apresentar os principais riscos e maneiras de mitigá-los.

Levantar os pré-requisitos necessários para o início do projeto.

As informações contidas no Plano de Implantação da Solução deverão ser escritas de maneira clara e objetiva, assim como os serviços propostos.

No cronograma, para cada fase do projeto, deverão indicar os dias necessários para as atividades contidas na fase.

As atividades deverão ser realizadas nos dias e horários explícitos no cronograma, podendo contemplar dias não úteis, com supervisão técnica de pelo menos 01 (um) responsável da CONTRATANTE, havendo necessidade de validação do responsável técnico da CONTRATADA.

Sempre que houver alteração do cronograma, uma nova versão deverá ser imediatamente encaminhada à CONTRATANTE, com respectivo relatório de impacto, e justificativa da mudança, que será ou não aceito, a critério da CONTRATANTE.

Qualquer alteração no corpo técnico ou gerencial da CONTRATADA não poderá afetar o cronograma, tampouco a qualidade dos produtos contratados.

A CONTRATADA deverá realizar a transferência de conhecimento da instalação dos equipamentos e acessórios contento, no mínimo, os seguintes tópicos: **Características do equipamento, Conceitos de Zona, Objetos e NAT, Balanceamento e Alta disponibilidade de *Link* WAN, Roteamento Inteligente, Conceitos de VPN,VPN *Site* a *Site* e *Client* to Site, VPN Baseado em Roteamento, SSL VPN, Métodos de autenticação suportados pelo Appliance, Filtro de Navegação, Autenticação única através de *Single* *Sign*-*On*, Integração com *Active* *Directory*, UTM (Gerenciamento Unificado de Ameaças),Discutindo Conceitos de Antivírus de Gateway , IPS (Serviço de Prevenção de Intrusos), *Firewall* de Aplicações**. Esse material deverá ser entregue em mídia.

A CONTRATADA deverá elaborar, depois de finalizados os trabalhos, e para o aceite final, relatório final com 01 cópia impressa e também 01 cópia em CD-ROM/DVD-ROM, apresentando no mínimo os seguintes itens:

* Confirmação de todos os requisitos necessários para o perfeito funcionamento dos serviços, e do hardware;
* Confirmação da presença de softwares, manual de instalação, manual de operação, e manual de manutenção;
* Documentação de todas as configurações efetuadas na solução, assim como todas as regras configuradas – *As-built*;
* Confirmação do perfeito funcionamento do hardware e do software para a solução como um todo;
* A identificação da instalação, cabeamento, etiquetagem, condições das tensões de alimentação e demais informações identificadoras da instalação;
* Cópia do Termo de Aceite Final do Projeto.

A CONTRATADA deverá concluir o projeto (instalação, configuração e integração) dentro do prazo máximo de 30 dias corridos, contados a partir da entrega dos Equipamentos e Softwares que compõem a solução, sem interrupção dos serviços ativos na CONTRATANTE.

1. **– SUPORTE TÉCNICO 24x7**

A CONTRATADA obriga-se a garantir a qualidade da solução implantada e a realização dos serviços de suporte técnico pelo prazo de 36 meses, a contar da implantação total do projeto.

A CONTRATADA ficará obrigada a garantir e a prestar assistência técnica, sem custos adicionais, contra defeitos de fabricação, pelo prazo de 36 meses a contar da implantação total do projeto.

O suporte técnico será acionado em caso de qualquer indisponibilidade da solução devendo ter como objetivos de atendimento os índices de criticidade a seguir:

|  |  |  |  |
| --- | --- | --- | --- |
| Criticidade | Descrição | Atendimento | Tempo de solução |
| Severidade 1 (Alta) | Sistema parado ou produto inoperante com impacto nas operações críticas de negócio. Parte substancial dos dados essenciais corre risco de perda ou corrupção. Operações relacionadas ao negócio foram afetadas, falha que compromete a integridade geral do sistema ou dos dados. Exemplo: serviço inativo, por falha ou configuração de Software | Em até 1 hora.24x7 | Em até 03 horas |
| Severidade 2(Média/Alta) | Alto impacto no ambiente de produção ou grande restrição de funcionalidade.Ocorreu um problema no qual um recurso importante foi gravemente danificado.As operações podem continuar de forma limitada, embora a produtividade, a curto prazo, possa ser afetada negativamente.Exemplo: Servidor não responde a comandos ou respondecom resultados inesperados. | Em até 2 horas 24x7 | Em até 04 horas |
| Severidade 3 (Baixa) | Demais problemas que não afetem diretamente o ambiente de produção. | No mesmo dia ou no próximo dia útil comercial | Em até 24 horas |

Deve possibilitar a abertura de chamados de suporte, para no mínimo, os seguintes métodos: via telefone (0800 ou ligação local São Paulo), ou via e-mail.

Todos os prazos para atendimento começarão a ser contados a partir da abertura do chamado, independentemente deste ter sido feito via telefone, ou via e-mail.

Considera-se plenamente solucionado o problema quando restabelecidos os sistemas/serviços sem restrições.

Os serviços de atendimento para chamados de severidades 1 e 2 não podem ser interrompidos até o completo restabelecimento de todas as funções do sistema paralisado (indisponível), mesmo que para isso tenham que se estender por períodos noturnos e dias não úteis (sábados, domingos e feriados).

Nos casos em que as manutenções necessitarem de paradas da solução, o CONTRATANTE deverá ser imediatamente notificado para que se proceda à aprovação da manutenção, ou para que seja agendada nova data, a ser definida pelo CONTRATANTE, para execução das atividades de manutenção.

1. **– BANCO DE HORAS**

A CONTRATANTE poderá solicitar suporte quando da necessidade de aprimoramento da solução, ou adequação de novos versionamentos, ou qualquer outra necessidade que não conste do escopo final do projeto, sendo que a quantidade de horas utilizadas será previa e formalmente ajustada entre o TCMSP e a CONTRATADA, e serão utilizadas as horas previstas abaixo, as quais serão faturadas pela CONTRATADA no mês seguinte à sua efetiva utilização:

* 70 (setenta) horas técnicas a serem prestadas em horário comercial, de segunda a sexta-feira;
* 80 (oitenta) horas técnicas a serem prestadas fora do horário comercial, inclusive sábados, domingos e feriados.

Os serviços serão prestados em conformidade com as ordens de serviços (OS) a serem emitidas para sua execução. As Ordens de Serviço poderão atender demandas pontuais ou serviços continuados, de acordo com planejamento realizado pela equipe do TRIBUNAL DE CONTAS DO MUNICIPIO DE SÃO PAULO, em conjunto com a equipe da CONTRATADA.

Toda solicitação, via e-mail ou contato telefônico, de Suporte deverá ser retornada no prazo máximo de 24 horas após o seu respectivo registro, entendido este retorno como um contato inicial para fins de definição da forma de tratamento da demanda apresentada, e a respectiva Ordem de Serviço.

Todas as funções e atividades desempenhadas pela empresa CONTRATADA deverão ter como preocupação primária, a transferência do conhecimento à equipe técnica do TRIBUNAL DE CONTAS DO MUNICIPIO DE SÃO PAULO designada a acompanhar cada atividade.

Entende-se por transferência de conhecimento, a passagem de conhecimento técnico para os técnicos do TRIBUNAL DE CONTAS DO MUNICIPIO DE SÃO PAULO, de todas as atividades desenvolvidas, relativas a cada Ordem de Serviço executada, visando aprimorar os conhecimentos da tecnologia utilizada e maximizar a utilização das funcionalidades.

1. **– TREINAMENTOS**

A CONTRATADA deverá fornecer ***Vouchers* de Treinamento**, com validade de 12 meses, para cursos oficiais, equivalentes aos módulos básico, intermediário e avançado, necessários para a implantação, operação, manutenção e configuração das funcionalidades da Solução adquirida, para a capacitação de 02 servidores do TCMSP, a serem ministrados pelo fabricante, ou por parceiros credenciados.

**ANEXO II**

**MODELO DE DECLARAÇÃO SOBRE TRIBUTOS MUNICIPAIS**

Processo: TC/011017/2019

Pregão nº 18/2019

**Ao**

**TRIBUNAL DE CONTAS DO MUNICÍPIO DE SÃO PAULO**

Aempresa.........................................................................,C.N.P.J. nº................................., **DECLARA**, sob as penas da lei e por ser a expressão da verdade, que não está cadastrada e não possui débitos junto à Fazenda do Município de São Paulo, relativamente aos tributos mobiliários.

**..................., de de 2019**

**Assinatura do Responsável pela Empresa**

(Nome Legível/Cargo/Carimbo do CNPJ)

**OBS.: 1- esta declaração deverá ser no original.**

 **2- apresentar na Habilitação – subitem 9.5.7.2 do Edital**

**ANEXO III**

**MODELO DE DECLARAÇÃO DE ME/EPP E INEXISTÊNCIA DE FATOS SUPERVENIENTES**

Processo: TC/011017/2019

Pregão nº 18/2019

A empresa ............................................................................................, inscrita no CNPJ sob nº.........................................................., por intermédio de seu representante legal infra-assinado, Sr(a). ......................................................................................,portador(a) da Carteira de Identidade nº................................. e do CPF nº ......................................., **DECLARA**, sob as penas do artigo 299 do Código Penal, **que se enquadra na situação de microempresa ou empresa de pequeno porte**, nos termos da Lei Complementar 123/06, bem como que inexistem fatos supervenientes que conduzam ao seu desenquadramento desta situação.

São Paulo, \_\_\_\_ de \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ de 2019.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Assinatura do responsável pela empresa proponente

Nome Legível:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

RG:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Cargo:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Empresa:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* **Obs. A declaração de ME/EPP deverá ser apresentada, SE CABÍVEL, no momento da HABILITAÇÃO (subitem 9.8.1 do Edital).**

**ANEXO IV**

**MODELO DE PROPOSTA COMERCIAL**

**(A SER PREENCHIDA PELA EMPRESA CLASSIFICADA EM PRIMEIRO LUGAR)**

Ao Tribunal de Contas do Município de São Paulo

Endereço: Av. Professor Ascendino Reis 1.130, São Paulo

Processo: TC/011017/2019

Pregão nº 18/2019

Abertura dia 20/09/2019 às 09 horas.

A \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_empresa estabelecida\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_nº\_\_\_, complemento:\_\_\_\_\_\_\_\_CNPJ. nº\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ telefone:\_\_\_\_\_\_\_e fax:\_\_\_\_\_\_\_\_\_\_\_\_,Bairro:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, Cidade:\_\_\_\_\_\_\_\_\_\_\_\_, Estado:\_\_\_, por meio de seu representante legal, Sr.(a) \_\_\_\_\_\_\_\_\_\_\_\_, \_\_\_\_\_\_\_\_\_\_\_\_(estado civil),\_\_\_\_\_\_\_\_\_\_\_(profissão) , portador(a) do RG nº \_\_\_\_\_\_\_\_\_\_\_\_\_\_ e CPF nº\_\_\_\_\_\_\_\_\_\_\_\_\_\_, **observadas as especificações constantes do Anexo I do Edital,** propõe o seguinte:

|  |
| --- |
| **SOLUÇÃO** |
| **Item** | **Qtde.** | **Descrição** | **Garantia** | **Valor unitário** | **Total** |
| 01 | 01 | FIREWALL UTM/NGFW do tipo *Appliance*, com Fonte Redundante, *Cluster*, Licenças, Solução Virtual de Relatórios, Instalação, Configuração e Suporte Técnico 24x7 | 36 meses | R$ | R$ |
| **BANCO DE HORAS** |
| **Item** | **Qtde.** | **Descrição** | **Período** | **Valor unitário** | **Total** |
| 02 | 70 horas | Suporte nos dias úteis entre 9h e 18h | 36 meses | R$ | R$ |
| 03 | 80 horas | Suporte nos demais horários | 36 meses | R$ | R$ |
| **TREINAMENTO** |
| **Item** | **Qtde.** | **Descrição** | **Validade** | **Valor unitário** | **Total** |
| 04 | 02 Servidores | *Vouchers* | 12 meses | R$ | R$ |

|  |
| --- |
| ‘ |
| **Valor total por extenso** |

**VALIDADE DA PROPOSTA:** Será de \_\_\_\_\_\_\_\_ dias contados a partir da data de abertura do envelope. (mínimo de 60 dias)

**CONDIÇÕES DE PAGAMENTO:** Conforme disposto na Minuta de Contrato – Anexo V.

**PRAZO DE ENTREGA:** conforme Minuta de Contrato – Anexo V.

Indicação do banco, número da conta e agência do licitante.

 Declaramos conhecer e nos submeter integralmente a todas as cláusulas e condições do Edital de Licitação do qual esta proposta é parte integrante.

São Paulo, \_\_\_\_\_\_ de \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ de 2019.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Assinatura do responsável da firma proponente)

Nome:/RG ----------------------------------------------------------------------

**ANEXO V**

**MINUTA DE CONTRATO**

|  |  |
| --- | --- |
| TERMO DE CONTRATO: | Nº  |
| CONTRATANTE: | TRIBUNAL DE CONTAS DO MUNICÍPIO DE SÃO PAULO |
| CONTRATADA: | <DENOMINAÇÃO SOCIAL DA EMPRESA> |
| OBJETO DO CONTRATO: | Aquisição de Solução, em Alta Disponibilidade, de FIREWALL UTM/NGFW do tipo Appliance, com Fonte Redundante e Cluster, incluindo Hardware, Software, Banco de Horas, Vouchers de Treinamento, Serviços de Instalação, Configuração e Suporte Técnico 24x7. |
| **VIGÊNCIA:** |  **36 (trinta e seis) meses** |
| DOTAÇÕES: | 77.10.01.032.3014.2818.4490.5210.10.01.032.3024.2818.3390.40 |
| VALOR CONTRATUAL: | R$ <\_\_\_\_\_\_\_\_\_\_,\_\_> |
| PROCESSO TC: | Nº 011017/2019 |

O TRIBUNAL DE CONTAS DO MUNICÍPIO DE SÃO PAULO, CNPJ nº 50.176.270/0001-26, com endereço na Av. Prof. Ascendino Reis, 1.130 – São Paulo/SP, neste ato representado por seu Presidente, JOÃO ANTONIO DA SILVA FILHO, doravante denominado CONTRATANTE, e <DENOMINAÇÃO SOCIAL DA EMPRESA>, CNPJ nº <\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_>, com endereço na <endereço da empresa>, doravante denominada CONTRATADA, neste ato representada por seu <cargo do representante da empresa>, <NOME DO REPRESENTANTE DA EMPRESA>, RG nº <\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_> e CPF nº <\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_>, conforme autorização constante do processo em epígrafe, resolvem celebrar este Contrato, decorrente da licitação na modalidade Pregão Eletrônico nº 18/2019 que se regerá pela legislação sobre licitações e contratos, particularmente a Lei Municipal 13.278/02, Decretos Municipais 44.279/03 e 46.662/05 e, no tocante às normas gerais e penais, pelas Leis Federais 8.666/93 e 10.520/02 e as cláusulas contratuais e condições que seguem:

**CLÁUSULA PRIMEIRA - DO OBJETO**: Aquisição de Solução, em Alta Disponibilidade, de FIREWALL UTM/NGFW do tipo Appliance, com Fonte Redundante e Cluster, incluindo Hardware, Software, Banco de Horas, Vouchers de Treinamento, Serviços de Instalação, Configuração e Suporte Técnico 24x7, conforme especificados no Termo de Referência, o qual passa a integrar este Contrato.

1.1 – Produtos objeto deste Contrato:

|  |
| --- |
| **SOLUÇÃO** |
| **Item** | **Qtde.** | **Descrição** | **Garantia** |
| 01 | 01 | FIREWALL UTM/NGFW do tipo Appliance, com Fonte Redundante, Cluster, Licenças, Solução Virtual de Relatórios, Instalação, Configuração e Suporte Técnico 24x7 | 36 meses |
| **BANCO DE HORAS** |
| **Item** | **Qtde.** | **Descrição** | **Período** |
| 02 | 70 horas | Suporte nos dias úteis entre 9h e 18h | 36 meses |
| 03 | 80 horas | Suporte nos demais dias e horários | 36 meses |
| **TREINAMENTO** |
| **Item** | **Qtde.** | **Descrição** | **Validade** |
| 04 | 02 servidores | Vouchers | 12 meses |

**CLÁUSULA SEGUNDA - DA VIGÊNCIA E DOS PRAZOS**

2.1 – O Contrato terá início de vigência a partir da data da sua assinatura e término na data da lavratura do termo de recebimento definitivo.

2.2 – Os Equipamentos e Softwares que compõem a Solução deverão ser entregues em até 60 (sessenta) dias após a data de emissão da Ordem de Fornecimento.

2.3 – Os Serviços de Implementação deverão ser finalizados em até 30 (trinta) dias após a entrega dos Equipamentos e Softwares.

2.3.1 – Os Serviços de Implementação deverão ser executados de forma a não comprometer os ambientes de produção durante o período de funcionamento do CONTRATANTE, ou seja, de segunda a sexta, das 7 às 19 horas.

2.4 – Os Vouchers de Treinamento deverão ser disponibilizados em até 20 (vinte) dias após a entrega da Solução.

2.5 – Os Equipamentos e Softwares que compõem a Solução terão garantia de 36 (trinta e seis) meses, contados a partir finalização dos Serviços de Implementação.

2.6 – O Banco de Horas – suporte nos dias úteis e demais dias – será utilizado pelo período de 36 (trinta e seis) meses, contados a partir da finalização dos Serviços de Implementação.

2.7 – Os Vouchers de Treinamento serão utilizados em até 12 (doze) meses, contados da disponibilização ao CONTRATANTE.

**CLÁUSULA TERCEIRA - DO PREÇO E CONDIÇÕES DE PAGAMENTO**:

3.1 - O valor contratual é de R<\_\_\_\_\_\_\_,\_\_> <(valor por extenso)>.

3.1.1 - Os preços a serem praticados serão os seguintes:

|  |
| --- |
| **SOLUÇÃO** |
| **Item** | **Qtde.** | **Descrição** | **Garantia** | **Valor Unitário** | **Valor Total** |
| 01 | 01 | FIREWALL UTM/NGFW do tipo Appliance, com Fonte Redundante, Cluster, Licenças, Solução Virtual de Relatórios, Instalação, Configuração e Suporte Técnico 24x7 | 36 meses | R$ | R$ |
| **BANCO DE HORAS** |
| **Item** | **Qtde.** | **Descrição** | **Período** | **Valor Unitário** | **Valor Total** |
| 02 | 70 horas | Suporte nos dias úteis entre 9h e 18h | 36 meses |  |  |
| 03 | 80 horas | Suporte nos demais dias e horários | 36 meses |  |  |
| **TREINAMENTO** |
| **Item** | **Qtde.** | **Descrição** | **Validade** | **Valor Unitário** | **Valor Total** |
| 04 | 02 servidores | Vouchers | 12 meses |  |  |
| **VALOR TOTAL:** |  |

3.2 - O pagamento relativo aos Equipamentos e Softwares que compõem a Solução será efetivado em até 15 (quinze) dias, após a finalização da entrega.

3.3 – O pagamento relativo ao Treinamento será efetivado em até 15 (quinze) dias após a sua realização.

3.4 – O pagamento relativo ao Banco de Horas será efetivado em até 15 (quinze) dias, depois de faturado pela CONTRATADA, no mês seguinte à efetiva utilização da(s) hora(s).

3.5 - Os pagamentos serão realizados através de depósito em conta corrente ou ficha de compensação, ambas de titularidade da CONTRATADA, mediante recibo expedido pelo responsável pela fiscalização do instrumento contratual, a ser indicado por autoridade competente, desde que cumpridas todas as exigências legais e contratuais pela CONTRATADA.

3.6 - Antes do pagamento, o CONTRATANTE efetuará consulta ao Cadastro Informativo Municipal – CADIN.

3.6.1 - A existência de registro no CADIN impede a realização de pagamento, conforme estabelecido no inciso II, art. 3º, da Lei nº 14.094/2005.

3.7 - O pagamento efetuado com atraso por culpa exclusiva do CONTRATANTE, terá o valor do principal reajustado pelo índice de remuneração básica da caderneta de poupança e de juros simples no mesmo percentual de juros incidentes sobre a caderneta de poupança para fins de compensação da mora (TR + 0,5% “pro-rata tempore”), observando-se, para tanto, o período correspondente à data prevista para o pagamento e aquela data em que o pagamento efetivamente ocorrer (conforme Portaria 05/2012-SF).

3.7.1 - Na hipótese de erro ou divergência com as condições contratadas, a nota fiscal/fatura será recusada pelo CONTRATANTEmediante declaração expressa das razões da desconformidade, ficando estabelecido que o prazo para pagamento seja contado a partir da data da apresentação da nova fatura devidamente corrigida.

**CLÁUSULA QUARTA - DOS RECURSOS ORÇAMENTÁRIOS**: As despesas resultantes do presente instrumento correrão por conta dos recursos constantes das dotações orçamentárias 77.10.01.032.3014.2818.4490.52 – Equipamentos e Material Permanente e 10.10.01.032.3024.2818.3390.40 - Serviços de Tecnologia da Informação e Comunicação – Pessoa Jurídica e, no próximo exercício, à conta das dotações orçamentárias previstas para atender despesas da mesma natureza.

**CLÁUSULA QUINTA - DOS DIREITOS E RESPONSABILIDADES DA CONTRATADA**:

5.1 - Executar o objeto na forma estabelecida no Termo de Referência - Anexo I do Edital.

5.2 - Manter o mais completo e absoluto sigilo sobre quaisquer dados, informações, documentos, especificações técnicas ou comerciais da CONTRATANTE, dos quais venha a ter conhecimento ou acesso, ou mesmo, venham a lhe ser confiados em razão desta contratação, não podendo, sob qualquer pretexto, reproduzir, utilizar ou deles dar conhecimento a terceiros estranhos a presente contratação sob as penas da Lei, mesmo após a rescisão deste Contrato.

5.3 - Manter atualizadas, durante a vigência da contratação, todas as condições de habilitação e qualificação exigidas para esta contratação, inclusive seus dados cadastrais.

5.4 - Responsabilizar-se pelo recolhimento de todos os tributos previstos na legislação vigente que incidam sobre o objeto contratado.

**CLÁUSULA SEXTA- DOS DIREITOS E RESPONSABILIDADES DO CONTRATANTE:**

6.1 **-** Caberá ao responsável pela fiscalização do Contrato a ser indicado por autoridade competente, na forma do artigo 67 da Lei Federal 8.666/93:

6.1.1 - Emitir a Ordem de Fornecimento;

6.1.2 - Acompanhar e supervisionar a realização dos serviços pelos técnicos da CONTRATADA;

6.1.3 - Prestar as informações e os esclarecimentos que venham a ser solicitados pelos técnicos da CONTRATADA;

6.1.4 - Exigir, a qualquer tempo, a comprovação das condições da CONTRATADA que ensejaram sua contratação, notadamente no tocante à qualificação técnica;

6.1.5 - Propor à autoridade competente a aplicação de penalidades, mediante caracterização da infração imputada à CONTRATADA, como disposto no art. 54 do Decreto Municipal nº 44.279/03;

6.1.6 - Propor à autoridade competente a dispensa de aplicação de penalidades à CONTRATADA, como disposto no art. 56 do Decreto Municipal nº 44.279/03;

6.1.7 - Receber provisoriamente o objeto, na forma disposta no artigo 73 da Lei Federal nº 8.666/93 e demais normas pertinentes;

6.1.8 - Receber definitivamente o objeto, mediante termo circunstanciado, após o decurso do prazo de observação ou vistoria que comprove a adequação do objeto aos termos contratuais, observado o disposto no artigo 69 da Lei Federal 8.666/93;

6.1.9 - Comunicar à CONTRATADA quaisquer irregularidades que porventura venha a constatar na execução dos serviços, sob os aspectos técnico e qualitativo, determinando o que julgar necessário à sua regularização.

**CLÁUSULA SÉTIMA - DAS PENALIDADES:**

7.1 - Odescumprimento das obrigações previstas em Lei ou neste Contrato sujeitará a CONTRATADA às seguintes multas, que poderão ser aplicadas em conjunto com as demais sanções dispostas na Seção II, do Capítulo IV, da Lei Federal 8.666/93 e art. 7º da Lei Federal 10.520/02:

7.1.1 – Advertência, que será aplicada em caso de faltas leves, eventos secundários, que não prejudiquem a execução do Contrato;

7.1.2 - Multa de 1% (um por cento) por dia de atraso no fornecimento do objeto, limitado a 10 (dez) dias úteis, após o que o fornecimento será considerado como definitivamente não realizado, implicando multa de 20% (vinte por cento), ambas calculadas sobre o valor da parcela inadimplida, salvo se houver motivo de força maior ou caso fortuito, justificado e aceito a critério exclusivo do CONTRATANTE;

7.1.3 - Multa de 1% (um por cento) por dia, constatado o descumprimento de obrigações relacionadas neste Contrato e no Termo de Referência, o qual figura como anexo deste ajuste, limitada a 10 (dez) dias, calculada sobre o valor total do ajuste, salvo se houver motivo de força maior ou caso fortuito, justificado e aceito a critério exclusivo do CONTRATANTE;

7.1.4 - Multa de 10% (dez por cento) do valor total deste instrumento, caso a CONTRATADA dê causa à rescisão do ajuste sem motivo justificado e aceito pelo CONTRATANTE.

7.2 - As multas são independentes, ou seja, a aplicação de uma não exclui a das outras, devendo ser recolhidas ou descontadas de pagamentos eventualmente devidos pelo CONTRATANTE em até 5 (cinco) dias úteis contados a partir de sua comunicação à CONTRATADA ou, ainda, se for o caso, cobradas judicialmente.

7.2.1 - O não recolhimento das multas no prazo implicará atualização monetária e juros moratórios calculados em conformidade com a Lei Municipal 13.275/2002.

7.3 - No caso de aplicação de eventuais penalidades será observado o procedimento previsto no Capítulo X do Decreto Municipal nº 44.279/03 e na Seção II do Capítulo 4 da Lei Federal nº 8.666/93

**CLÁUSULA OITAVA - DA ANTICORRUPÇÃO:** Para a execução deste contrato, nenhuma das partes poderá oferecer, dar ou se comprometer a dar a quem quer que seja, ou aceitar ou se comprometer a aceitar de quem quer que seja, tanto por conta própria quanto por intermédio de outrem, qualquer pagamento, doação, compensação, vantagens financeiras ou não financeiras ou benefícios de qualquer espécie que constituam prática ilegal ou de corrupção, seja de forma direta ou indireta quanto ao objeto deste contrato, ou de outra forma a ele não relacionada, devendo garantir, ainda, que seus prepostos e colaboradores ajam da mesma forma, conforme disposto no Decreto Municipal n° 56.633/2015.

**CLÁUSULA NONA - DA RESCISÃO:** O ajuste poderá ser rescindido, independentemente de interpelação judicial ou extrajudicial, nas hipóteses previstas na Lei Municipal 13.278/02, Decreto Municipal 44.279/03 e da Lei Federal 8.666/93.

**CLÁUSULA DÉCIMA - DA LEGISLAÇÃO APLICÁVEL:** Lei Federal 8.666/93 e 10.520/02, Lei Municipal 13.278/02, Decretos Municipais 44.279/03 e 46.662/05 e legislação correlata, aplicando-se, quando for o caso, supletivamente, os princípios da Teoria Geral dos Contratos e as disposições do Direito Privado.

**CLÁUSULA DÉCIMA PRIMEIRA –** **DO FORO:** Fica eleito o Foro da Comarca desta Capital para solução de quaisquer litígios relativos ao presente ajuste, com renúncia expressa de qualquer outro por mais privilegiado que seja.

E, por estarem de acordo, as partes firmam este contrato, em duas vias de igual teor.

São Paulo,

|  |  |  |
| --- | --- | --- |
| **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_****JOÃO ANTONIO DA SILVA FILHO**Presidente**TRIBUNAL DE CONTAS DO MUNICÍPIO DE SÃO PAULO** |  | **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_****<NOME DO REPRESENTANTE>**<Cargo do representante>**<DENOMINAÇÃO SOCIAL DA EMPRESA>** |