PREFEITURA DO MUNICÍPIO DE BASTOS
ESTADO DE SÃO PAULO

EDITAL MINUCIOSO

PREGÃO PRESENCIAL N.º 098/2019
PROCESSO ADMINISTRATIVO N.º 141/2019
DATA DA REALIZAÇÃO: 18/12/2018
HORÁRIO: 8:30 HS.
LOCAL: Divisão de Compras da PREFEITURA DO MUNICÍPIO DE BASTOS, sito à Rua Ademar de Barros, 530 – centro – Bastos – SP.

O Prefeito Municipal de Bastos Estado de São Paulo, no uso de suas atribuições legais, faz saber que se encontra aberto na Divisão de Licitações, o Edital de Pregão Presencial 098/2019, para a CONTRATAÇÃO DE EMPRESA ESPECIALIZADA PARA PRESTAÇÃO DE SERVIÇOS DE TELECOMUNICAÇÕES E TECNOLOGIA DA INFORMAÇÃO, SENDO ELES: (1) PRESTAÇÃO DE SERVIÇO DE TELECOMUNICAÇÕES STFC (SERVIÇO TELEFÔNICO FIXO COMUTADO) NAS MODALIDADES ANALÓGICO E DIGITAL, (2) FORNECIMENTO DE LINK DEDICADO DE ACESSO À INTERNET, (3) FORNECIMENTO E IMPLANTAÇÃO DE SOLUÇÃO DE SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO, NOS TERMOS DAS CONCESSÕES OUTORGADAS PELA AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES – ANATEL, pelo regime de execução por preço global, sendo o tipo de licitação a de MENOR PREÇO, regido em todos os seus termos pelas Leis Federais n.ºs 10.520 de 17 de julho de 2002, 8.666/93 de 23 de junho de 1993 alterada pela Lei Federal n.º 8.883/94 e introduções posteriores, Lei Municipal n.º 1.980/07 de 16 de outubro de 2007, Decreto nº597/09 de 26 de janeiro de 2009, Lei Complementar 123/2006, alterada pela Complementar nº147, de 7 de agosto de 2.014e demais normas regulamentares aplicáveis à espécie. Os envelopes contendo a proposta e os documentos de habilitação serão recebidos no endereço acima mencionado, na sessão pública de processamento do Pregão, após o credenciamento dos interessados que se apresentarem para participar do certame.

A sessão do processamento do pregão será realizada na Divisão de Compras da PREFEITURA DO MUNICÍPIO DE BASTOS, sito à Rua Ademar de Barros, 530 – centro Bastos - SP, no dia 18 de dezembro de 2019, no horário das 8:30hs., será realizada pelo Pregoeiro e Equipe de Apoio, designados nos autos do processo em epígrafe através de Portaria.

1.0 - DO OBJETO:

CONTRATAÇÃO DE EMPRESA ESPECIALIZADA PARA PRESTAÇÃO DE SERVIÇOS DE TELECOMUNICAÇÕES E TECNOLOGIA DA INFORMAÇÃO, SENDO ELES: (1) PRESTAÇÃO DE SERVIÇO DE TELECOMUNICAÇÕES STFC (SERVIÇO TELEFÔNICO FIXO COMUTADO) NAS MODALIDADES ANALÓGICO E DIGITAL, (2) FORNECIMENTO DE LINK DEDICADO DE ACESSO À INTERNET, (3) FORNECIMENTO E IMPLANTAÇÃO DE SOLUÇÃO DE SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO, NOS TERMOS DAS CONCESSÕES OUTORGADAS PELA AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES – ANATEL, a seguir discriminados:-

PARECER
Examinado e aprovado pela Secretaria Mun.dos
Negócios Juridicos de acordo com a Lei 8.666/93
Atualizada pela Lei 8.883/94
Bastos-SP, 23 de outubro de 2019
Rafael Teixeira Sebastiani – OAB/SP 355751
Procurador Jurídico

ITEM	QTDE	UNID	DESCRIÇÃO
1	1	SERV	CONTRATAÇÃO DE EMPRESA ESPECIALIZADA PARA PRESTAÇÃO DE SERVIÇOS DE TELECOMUNICAÇÕES E TECNOLOGIA DA INFORMAÇÃO, SENDO ELES: (1) PRESTAÇÃO DE SERVIÇO DE TELECOMUNICAÇÕES STFC (SERVIÇO TELEFÔNICO FIXO COMUTADO) NAS MODALIDADES ANALÓGICO E DIGITAL, (2) FORNECIMENTO DE LINK DEDICADO DE ACESSO À INTERNET, (3) FORNECIMENTO E IMPLANTAÇÃO DE SOLUÇÃO DE SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO, NOS TERMOS DAS CONCESSÕES OUTORGADAS PELA AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES – ANATEL
	50	UNID	LINHAS CONVENCIONAIS
	2	UNID	TRONCOS DIGITAIS 10 CANAIS
	10	UNID	RAMAIS DDR PARA SECRETARIA MUNICIPAL DE EDUCAÇÃO
	10	UNID	RAMAIS DDR PARA FUNDO MUNICIPAL DE SAÚDE
	1	UNID	TRONCO DIGITAL DE 15 CANAIS
	15	UNID	RAMAIS DDR PARA PREFEITURA
	1	UNID	PACOTE DE MINUTOS ILIMITADO NACIONAL COM 15 RAMAIS
	2	UNID	PACOTE DE MINUTOS ILIMITADO NACIONAL COM 10 RAMAIS
	1	UNID	INTERNET DEDICADA 100 MB COM SEGURANÇA
	7	UNID	INTERNET BANDA LARGA
			LIGAÇÕES LOCAIS
	7.000		MINUTO FIXO - FIXO (LOCAL) TERMINAL
	1.000		MINUTO LOCAL (VC1) TERMINAL
	10.000		MINUTO FIXO - FIXO (LOCAL) DDR
	3.000		MINUTO LOCAL (VC1) DDR
			LIGAÇÕES DE LONGA DISTÂNCIA
	1.000		MINUTO FIXO - FIXO INTRA-REGIONAL
	100		MINUTO FIXO - MÓVEL INTRA-REGIONAL (VC2)
	100		MINUTO FIXO - FIXO INTER-REGIONAL
	10		MINUTO FIXO - MÓVEL INTER-REGIONAL (VC3)
	2.500		MINUTO FIXO - FIXO INTRA-REGIONAL TIPO DDR
	280		MINUTO FIXO - MÓVEL INTRA-REGIONAL (VC2) TIPO DDR
	120		MINUTO FIXO - FIXO INTER-REGIONAL TIPO DDR
	35		MINUTO FIXO - MÓVEL INTER-REGIONAL (VC3) TIPO DDR

2.0 - CONDIÇÕES DE PARTICIPAÇÃO:

Poderão participar do certame todos os interessados do ramo de atividade pertinente ao objeto desta licitação, que preencherem as condições de credenciamento e requisitos deste edital.

3.0 - DO CREDENCIAMENTO:

Para o credenciamento deverão ser apresentados os documentos a seguir discriminados:

Tratando-se de representante legal: o estatuto social, contrato social ou outro instrumento de registro comercial, registrado na Junta Comercial, no qual estejam expressos seus poderes para exercer direitos e assumir obrigações em decorrência da investidura. Tratando-se de procurador, o instrumento de procuração público ou particular com firma reconhecida do qual constem poderes específicos para formular

lances, negociar preço, interpor recursos e desistir de sua interposição e praticar todos os demais atos pertinentes ao certame, acompanhado do correspondente documento que comprove os poderes do mandante para a outorga.

O representante legal e o procurador deverão se identificar exibindo documento oficial de identificação que contenha foto.

Será admitido apenas 01 (um) representante para cada licitante credenciada, sendo que cada um deles poderá representar apenas uma credenciada.

A ausência do Credenciado, em qualquer momento da sessão, importará em imediata exclusão da licitante por ele representada, salvo autorização expressa do Pregoeiro.

3.1 – PARA AS EMPRESAS ME e EPP

Deverão apresentar declaração e comprovante de que se encontram na condição de ME ou EPP como descrito pela Lei Complementar nº 123/2006.

DECLARAÇÃO

Declaro para fins de participação no Pregão Presencial nº 098/2019 que a empresa ..... (Nome da Empresa), CNPJ ..... está sob o regime da Lei Complementar nº 123/2006, portanto goza do direito de preferência em caso de empate de preços. Por ser a expressão da verdade firmo a presente declaração para os efeitos legais.

Assinatura
Nome do representante de empresa

4.0 - DA FORMA DE APRESENTAÇÃO DA DECLARAÇÃO DE PLENO ATENDIMENTO AOS REQUISITOS DE HABILITAÇÃO, DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO.

A declaração de pleno atendimento aos requisitos de habilitação de acordo com o modelo abaixo deverá ser apresentada fora dos Envelopes n.ºs 1 e 2.

4.1 - MODELO

Eu (nome completo), representante legal da empresa (nome da pessoa jurídica), interessada em participar no Processo Licitatório n.º 141/19, na Modalidade Pregão (Presencial) n.º 098/2019, da Prefeitura do Município de Bastos/SP., declaro pleno atendimento aos requisitos de habilitação desta empresa.

Local e data.

Nome, RG e assinatura do representante legal.

A proposta e os documentos para habilitação deverão ser apresentados, separadamente em 2 envelopes fechados e indevassáveis, contendo em sua parte externa, além do nome da proponente, os seguintes dizeres:

ENVELOPE N.º 1 – PROPOSTA
Pregão n.º ..098/2019
Processo n.º ...141/19
Prefeitura do Município de Bastos/SP.

ENVELOPE N.º 2 – HABILITAÇÃO
Pregão n.º ...098/2019
Processo n.º ...141/19
Prefeitura do Município de Bastos/SP.

PARECER
Examinado e aprovado pela Secretaria Mun.dos
Negócios Juridicos de acordo com a Lei 8.666/93
Atualizada pela Lei 8.883/94
Bastos-SP, 23 de outubro de 2019
Rafael Teixeira Sebastiani – OAB/SP 355751
Procurador Jurídico

4.2 - A proposta deverá ser elaborada em papel timbrado da empresa e redigida em língua portuguesa, salvo quanto às expressões técnicas de uso corrente, com suas páginas numeradas seqüencialmente, sem rasuras, emendas, borrões ou entrelinhas e ser datada e assinada pelo representante legal da licitante ou pelo procurador, juntando-se a procuração.

Os documentos necessários à habilitação deverão ser apresentados em original, por qualquer processo de cópia autenticada por tabelião de notas ou cópia acompanhada do original para autenticação pelo Pregoeiro ou por membro da Equipe de Apoio.

5.0 - DO CONTEÚDO DO ENVELOPE PROPOSTA

A proposta de preço deverá conter os seguintes elementos:

Nome, endereço, CNPJ e inscrição estadual/municipal da licitante, se houver;
Número do processo e do Pregão;

Descrição do objeto da presente licitação, inclusive marca, em conformidade com as especificações do folheto descritivo;

Preço unitário e total, por item em moeda corrente nacional, em algarismo, apurado à data de sua apresentação, sem inclusão de qualquer encargo financeiro ou previsão inflacionária. Nos preços propostos deverão estar incluídos, além do lucro, todas as despesas e custos, como por exemplo: transportes, tributos de qualquer natureza e todas as despesas, diretas ou indiretas, relacionadas com o fornecimento do objeto da presente licitação;

Prazo de validade da proposta não inferior a 60 (sessenta) dias.

6.0 - DO CONTEÚDO DO ENVELOPE "DOCUMENTOS PARA HABILITAÇÃO"

O Envelope "Documentos de Habilitação" deverá conter os documentos a seguir relacionados os quais dizem respeito a:

6.1 - HABILITAÇÃO JURÍDICA

Registro comercial, no caso de empresa individual;

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

Documentos de eleição dos atuais administradores, tratando-se de sociedades por ações, acompanhados da respectiva ata da última eleição;

Ato constitutivo devidamente registrado no Cartório de Registro Civil de Pessoas Jurídicas, tratando-se de sociedades civis, acompanhado de prova da diretoria em exercício;

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

Os documentos apresentados no credenciamento não precisarão constar do Envelope "Documentos de Habilitação", se tiverem sido apresentados para o credenciamento neste Pregão.

6.2 - DA REGULARIDADE FISCAL

Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas do Ministério da Fazenda (CNPJ);
Certidão de regularidade de débito com a Fazenda Estadual (relativos ao ICMS) da sede da licitante;
Certidão de regularidade de débito para com a Fazenda Municipal da sede da licitante;
Certidão de regularidade de débito para com o Sistema de Seguridade Social (INSS) e com o Fundo de Garantia por Tempo de Serviço (FGTS).
Certidão de regularidade de débito para com a Sec. da Receita Federal e a Procuradoria da Fazenda Nacional.
Certidão Negativa de Débitos Trabalhistas (CNDT).

6.3 - OUTRAS COMPROVAÇÕES

Declarações da licitante, elaborada em papel timbrado e subscrita por seu representante legal, de que se encontra em situação regular perante o **Ministério do Trabalho** e declaração que **não possui fato superveniente impeditivo**:

7.0 - MODELO DE SITUAÇÃO REGULAR PERANTE O MINISTÉRIO DO TRABALHO

Eu (nome completo), representante legal da empresa (nome da pessoal jurídica), interessada em participar do processo licitatório, na Modalidade Pregão (Presencial) n.º 098/2019 , da Prefeitura do Município de Bastos, declaro sob as penas da lei que a (nome da pessoa jurídica) encontra-se em situação regular perante o Ministério do trabalho, no que se refere à observância do disposto no inciso XXXIII, do artigo 7.º, da Constituição Federal.

Local e data.
Nome, RG e assinatura do representante legal.

Declaração elaborada em papel timbrado e subscrita pelo representante legal da licitante, assegurando a inexistência de impedimento legal para licitar ou contratar com a Administração.

7.1 – MODELO de Declaração de inexistência de fato superveniente impeditivo de habilitação, na forma do § 2º do artigo 32 da Lei Federal nº 8.666/93

MINUTA DE DECLARAÇÃO DE INEXISTÊNCIA DE FATO SUPERVENIENTE

Ref: (identificação da licitação)
....., inscrito no CNPJ nº ....., por intermédio de seu representante legal o(a) Sr(a)....., portador(a) da Carteira de Identidade nº ..... e do CPF nº .....DECLARA, para fins do disposto no § 2º do artigo 32 da Lei 8.666, de 21 de junho de 1993, acrescido pela Lei nº 9.854, de 27 de outubro de 1999, que não está impedida de participar de licitações ou contratar com a Administração Pública, Direta ou Indireta e que não é declarada inidônea pelo Poder Público, de quaisquer esferas da Federação. Não se encontra, nos termos da legislação em vigor ou do Pregão, sujeito a qualquer outro fato ou circunstância que possa impedir a sua regular participação na presente licitação, ou a eventual contratação que deste procedimento possa decorrer.
.....
(data)
.....
(assinatura do representante legal)

7.2 – As empresas deverão apresentar **TERMO DE AUTORIZAÇÃO OU DECLARAÇÃO DE QUE DETÉM A CONCESSÃO DADA PELA AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES (ANATEL) para prestação de serviço.**

8.0 - DAS DISPOSIÇÕES GERAIS DA HABILITAÇÃO

É facultada às licitantes a substituição dos documentos de habilitação exigidos neste Edital, pelo comprovante de registro cadastral da Prefeitura de Bastos, para participar de licitações junto ao Município de Bastos no ramo de

atividade compatível com o objeto do certame, o qual deverá ser apresentado acompanhado dos documentos relacionados nos subitens 6.2 e 6.3 do item 6, que não tenham sido apresentados para o cadastramento ou, se apresentados, já estejam com os respectivos prazos de validade vencidos na data de apresentação das propostas.

Na hipótese de não constar prazo de validade nas certidões/documentos apresentadas, a Administração aceitará como válidas as expedidas até 90 (noventa) dias imediatamente anteriores à data de apresentação das propostas.

9.0 - DO PROCEDIMENTO E DO JULGAMENTO

9.1 O procedimento de julgamento será o menor preço ou lance. Após esgotadas as etapas de lances, o pregoeiro Adjudicará o objeto a quem ofertar o menor lance ou preço.

No local, data e horário constantes do preâmbulo, será aberta a sessão de processamento do Pregão, iniciando-se com o credenciamento dos interessados em participar do certame, com duração mínima de 30 minutos.

Após o credenciamento, as licitantes entregarão ao Pregoeiro a declaração de pleno atendimento aos requisitos de habilitação, em envelopes separados, da proposta de preços e dos documentos de habilitação.

9.1.1 O Pregoeiro(a) procederá à abertura do Envelope I, contendo as Propostas de Preços, estas serão analisadas verificando o atendimento a todas as especificações e condições estabelecidas neste Edital e seus Anexos **(EXAME DE CONFORMIDADE)**, sendo imediatamente desclassificadas aquelas que estiverem em desacordo.

9.1.2 O Pregoeiro (a) classificará o autor da proposta de "**MENOR PREÇO",** e aqueles que tenham apresentado propostas em valores sucessivos ou superiores em até 10% (dez por cento), para participarem dos lances verbais;

9.1.3 Quando não forem verificadas, no mínimo, três propostas escritas nas condições do item acima, o pregoeiro classificará todas as propostas, quaisquer que sejam os preços oferecidos nas propostas escritas;

9.1.4 Aos licitantes classificados será dada oportunidade para disputa, por meio de lances verbais e sucessivos, em valor mínimo de R$ 1,00 (um real), a partir do autor da proposta classificada de maior preço.

9.1.5 O licitante que desistir de apresentar lance verbal, quando convocado pelo Pregoeiro, será excluído da etapa de lances verbais, mantendo-se o último preço apresentado pelo mesmo, para efeito de ordenação das propostas.

9.1.6 Caso não se realize lances verbais, serão verificados a conformidade entre a proposta escrita de menor preço e o valor estimado para a contratação.

9.1.7 No certame será assegurado, como critério de desempate, preferência de contratação para as microempresas (ME) e empresas de pequeno porte (EPP).

9.1.8 Entende-se por empate aquelas situações em que as propostas apresentadas pelas microempresas (ME) e empresas de pequeno porte (EPP) sejam iguais ou até 5% (cinco por cento) superiores à proposta mais bem classificada.

9.1.9 Para efeito do disposto no subitem 9.1.8, ocorrendo empate, proceder-se-á da seguinte forma:

9.2 A microempresa ou empresa pequeno porte mais bem classificada poderá apresentar proposta de preço inferior àquela considerada vencedora do certame, situação em que será adjudicado em seu favor o objeto licitado;

9.2.1 Não ocorrendo a contratação da microempresa ou empresa de pequeno porte, na forma do item 9.2, serão convocadas as remanescentes que porventura se enquadrem na hipótese do subitem 9.1.8, na ordem classificatória, para o exercício do mesmo direito;

9.2.2 No caso de equivalência dos valores apresentados pelas microempresas e empresas de pequeno porte que se encontrem no intervalo estabelecido no subitem 9.1.8, será realizado sorteio entre elas para que se identifique aquela que primeiro poderá apresentar melhor oferta.

9.2.3 Na hipótese da não contratação nos termos previstos no subitem 9.1.9, os objetos licitados serão adjudicados em favor da proposta originalmente vencedora do certame.

9.2.4 Os dispositivos estabelecidos no subitem 9.1.9 e complementos somente se aplicarão quando a melhor oferta inicial não tiver sido apresentada por microempresa ou empresa de pequeno porte.

9.2.5 A microempresa ou empresa de pequeno porte, melhor classificada será convocada para apresentar nova proposta no prazo máximo de 5 (cinco) minutos após o encerramento dos lances e solicitação do Pregoeiro, sob pena de preclusão.

9.2.6 Quando houver discrepância:

9.2.7 Entre os valores unitários e os totais resultantes de erros de multiplicação e quantidades por valores unitários prevalecerão os valores unitários e o valor total corrigidos;

9.2.8 Entre os valores dos subtotais e os totais, resultantes de erros de adição prevalecerão os valores dos subtotais corrigindo o valor total;

9.2.9. Dos dados ofertados nas propostas e nos anexos, prevalecerão os da proposta exceto nos casos em que os anexos forem mais vantajosos para a Administração Pública;

9.3 Se a oferta não for aceitável ou se o licitante desatender às exigências habilitatórias, o Pregoeiro examinará a oferta subseqüente, verificando a aceitabilidade e procedendo à habilitação do licitante, na ordem de classificação, e assim sucessivamente, até a apuração de uma proposta que atenda a todas as exigências, sendo o respectivo licitante declarado vencedor e a ele adjudicado a proposta do objeto licitado definido neste Edital e seus Anexos.

9.3.1 O Pregoeiro poderá negociar diretamente com o licitante para que seja obtido preço melhor.

9.3.2 Será de exclusiva responsabilidade da licitante, não lhe assistindo o direito de pleitear qualquer alteração, sob alegação de erro, omissão ou qualquer outro pretexto. Contudo, se a licitante for classificada na sessão do Pregão para ofertar lances verbais, poderá fazê-lo na forma e oportunidade previstas neste Edital;

9.3.3 A licitante vencedora, após a etapa de lances, deverá assinar a ata constando o valor final negociado.

9.3.4 Da reunião lavrar-se-á ata circunstanciada, na qual serão registradas as ocorrências relevantes e que, ao final, deverá obrigatoriamente ser assinada pelo Pregoeiro e o(s) licitante(s) presente(s).

9.3.5 Não se considerará qualquer oferta de vantagem não prevista neste Edital e seus Anexos.

9.3.6 Serão desclassificadas as propostas que não atenderem às exigências do presente Edital e seus Anexos, sejam omissas ou apresentem irregularidades, ou defeitos capazes de dificultar o julgamento. E ainda as que apresentarem preços manifestadamente inexeqüíveis ou excessivos.

10. - DO RECURSO, DA ADJUDICAÇÃO E DA HOMOLOGAÇÃO.

10.1 - No final da sessão, a licitante que quiser recorrer deverá manifestar imediata e motivadamente a sua intenção, abrindo-se então o prazo de 3 (três) dias úteis para apresentação de memoriais, ficando as demais licitantes desde logo intimadas para apresentar contra-razões em igual número de dias, que começarão a correr no término do prazo do recorrente, sendo-lhes assegurada vista imediata dos autos.

10.2 - A ausência de manifestação imediata e motivada da licitante importará: a decadência do direito de recurso, a adjudicação do objeto do certame pelo Pregoeiro à licitante vencedora e o encaminhamento do processo à autoridade competente para homologação.

10.3 - Interposto o recurso, o Pregoeiro poderá reconsiderar a sua decisão ou encaminhá-lo devidamente informado à autoridade competente.

10.4 - Decididos os recursos e constatada a regularidade dos atos praticados, a autoridade competente adjudicará o objeto do certame à licitante vencedora e homologará o procedimento.

10.5 - O recurso terá efeito suspensivo e o seu acolhimento importara a invalidade apenas dos atos insuscetíveis de aproveitamento.

11 - DOS PRAZOS, DAS CONDIÇÕES E LOCAL DE ENTREGA DO OBJETO DA LICITAÇÃO.

Os serviços/produtos deverão ser entregues em no máximo 30 dias, após solicitação da Divisão de CPD..
Deverão ser entregues na PREFEITURA DO MUNICÍPIO DE BASTOS, sito à Rua Adhemar de Barros, nº 530 tel.:- (0xx14) 3478-9800, no horário das 8:00 às 10:00 hs e 13:00 às 16:00 hs., de segunda à sexta-feira.

11.1 - Correrão por conta da contratada todas as despesas de transportes, tributos, encargos trabalhistas e previdenciários, decorrentes da entrega e das mercadorias.

11.2 - Por ocasião da entrega, a Contratada deverá colher no comprovante respectivo a data, o nome, o cargo, a assinatura e o número do Registro Geral (RG), do servidor responsável pelo recebimento do objeto licitado.

12 - DA FORMA DE PAGAMENTO:

12.1 - O pagamento será efetivado no 10º dia útil do mês subsequente da entrega dos serviços e após a apresentação de fatura mensal ou nota fiscal, mediante a comprovação da CONTRATADA de sua regularidade com a Seguridade Social "INSS" e para com o "FGTS", sob pena do pagamento não ser efetuado. (O setor de tesouraria fará a pesquisa para comprovar a regularidade).

12.2 - Os pagamentos serão creditados em nome da contratada, mediante ordem bancária em conta corrente por ela indicada ou por meio de ordem bancária para pagamento de faturas com código de barras, uma vez satisfeitas as condições estabelecidas neste edital.

12.3 - Se por ocasião do pagamento as certidões de regularidade de débito da Adjudicatária perante o Sistema de Seguridade Social (INSS), o Fundo de Garantia por Tempo de Serviço (FGTS) e a Secretaria da Receita Federal e a Procuradoria Nacional, estiverem com os prazos de validade vencidos, o órgão licitante verificará a situação por meio eletrônico hábil de informações, certificando nos autos do processo a regularidade e anexando os documentos passíveis de obtenção por referidos meios, salvo impossibilidade devidamente justificada.

12.4 - Se não for possível atualizá-las por meio eletrônico hábil de informações a Adjudicatária será notificada para no prazo de 02 (dois) dias úteis, comprovar a sua situação de regularidade, mediante apresentação das certidões respectivas com prazo de validade em vigência sob pena da contratação não se realizar.

13 - DA CONTRATAÇÃO:

O contrato a ser assinado, terá validade até 12 meses, podendo ser prorrogado por iguais e sucessivos períodos até o limite de 60 meses, em caso de falta de quantitativo será aditado em até 25% da

quantidade inicial contratada nos termos do artigo 65, § 1º, da Lei n. 8.666/93, a quantidade excedente após o término do contrato será estornada.

A despesa onerará os recursos da seguinte dotação orçamentária:

Estado de São Paulo
Prefeitura Municipal de Bastos
Órgão 2 - Executivo

Modalidade:	**PREGÃO PRESENCIAL**	**Nº**	**098/19**
Objeto:	Classificação orçamentária com a categoria econômica funcional programática para contratação de empresa no ramo de telefonia fixa destinado a vários setores da municipalidade		

Despesa desdobrada	Natureza da despesa	Nomenclatura da Despesa	Funcional Programática	Unidade Orçamentária	Despesa Principal	Fonte	CA	Saldo da Dotação	Nome do Recurso
6409	33904004	COMUNICAÇÃO DE DADOS	02.01.00.04.122.0003.2.003	GABINETE DO PREFEITO E DEPENDÊNCIAS	621	1	110.0000	3.376,03	TESOURO
6346	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
6410	33904004	COMUNICAÇÃO DE DADOS	02.02.00.04.122.0004.2.004	SEC. MUN. DE ADMINISTRAÇÃO	696	1	110.0000	11.097,89	TESOURO
6347	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
7179	33904004	COMUNICAÇÃO DE DADOS	02.03.00.04.122.0006.2.008	MANUT. SEC. MUN. DE PLANEJAMENTO	2404	1	110.000	1.516,08	TESOURO
6348	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
6477	33904004	COMUNICAÇÃO DE DADOS	02.04.00.12.361.0014.2.014	SEC. MUN. DE EDUCAÇÃO E CULTURA - ENSINO FUNDAMENTAL	2445	1	2200000	9.044,95	TESOURO
6358	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
6478	33904004	COMUNICAÇÃO DE DADOS	02.04.00.12.365.0016.2.016	MANUT. ENSINO INFANTIL - PRÉ-ESCOLA	2446	1	213.0000	20.151,98	TESOURO
6359	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
6479	33904004	COMUNICAÇÃO DE DADOS	02.04.00.13.391.0027.2.049	MANUT. DO PATRIMÔNIO HISTÓRICO, ARTÍSTICO E ARQUEOLÓGICO	2447	1	110.0000	324,49	TESOURO
6360	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
6489	33904004	COMUNICAÇÃO DE DADOS	02.05.00.10.122.0047.2.074	MANUT. DA SEC. DE SAÚDE	716	1	310.0000	6.736,65	TESOURO

PARECER
Examinado e aprovado pela Secretaria Mun.dos
Negócios Juridicos de acordo com a Lei 8.666/93
Atualizada pela Lei 8.883/94
Bastos-SP, 23 de outubro de 2019
Rafael Teixeira Sebastiani – OAB/SP 355751
Procurador Jurídico

6349	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
6489	33904004	COMUNICAÇÃO DE DADOS	02.05.00.10.301.0037.2.017	MANUT. DO FUNDO MUN. DE SAÚDE	1915	2	300.0056	7.739,03	PAB
6350	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
6789	33904004	COMUNICAÇÃO DE DADOS	02.05.00.10.302.0017.2.120	PRONTO-SOCORRO MUNICIPAL	724	1	310.0000	1.484,94	TESOURO
6351	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
6480	33904004	COMUNICAÇÃO DE DADOS	02.06.00.27.812.0019.2.019	MANUT. DA SEC. MUN. DE ESPORTES	697	1	110.000	2.813,50	TESOURO
6352	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
7178	33904004	COMUNICAÇÃO DE DADOS	02.07.00.04.122.0004.2.020	MANUT. SEC. MUN. DOS NEGÓCIOS JURÍDICOS	1950	1	110.0000	300,00	TESOURO
6353	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
6481	33904004	COMUNICAÇÃO DE DADOS	02.08.00.08.244.0021.2.021	MANUT. SEC. DE PROMOÇÃO SOCIAL	698	1	510.0000	2.565,44	TESOURO
6354	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
6483	33904004	COMUNICAÇÃO DE DADOS	02.09.00.20.606.0026.2.026	MANUT. DA SEC. DE AGRICULTURA E MEIO AMBIENTE	717	1	110.0000	1.534,49	TESOURO
6355	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
6482	33904004	COMUNICAÇÃO DE DADOS	02.11.00.08.243.0024.2.025	MANUT. DO FUNDO MUN. DOS DIRETOS DA CRIANÇA E DO ADOLESCENTE	719	1	500.0003	2.468,41	TESOURO
6356	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
6479	33904004	COMUNICAÇÃO DE DADOS	02.12.00.23.695.0030.2.053	MANUT. DA SEC. DE TURISMO	718	1	110.0000	1.578,36	TESOURO
6357	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
Total de dotação disponível nesta data 23/10/2019:								**72.732,24**	

Neusa Kyoka Hitaka Nishida

Assessora Div. Contabilidade

R.G. 18.913.743-5 SSP/SP

PARECER
Examinado e aprovado pela Secretaria Mun.dos
Negócios Juridicos de acordo com a Lei 8.666/93
Atualizada pela Lei 8.883/94
Bastos-SP, 23 de outubro de 2019
Rafael Teixeira Sebastiani – OAB/SP 355751
Procurador Jurídico

Estado de São Paulo
Prefeitura Municipal de Bastos
Órgão 2 - Executivo

Modalidade:	**PREGÃO PRESENCIAL**	**Nº**	**098/19**
Objeto:	Classificação orçamentária com a categoria econômica funcional programática para contratação de empresa no ramo de telefonia fixa destinado a vários setores da municipalidade		

Despesa desdobrada	Natureza da despesa	Nomenclatura da Despesa	Funcional Programática	Unidade Orçamentária	Despesa Principal	Fonte	CA	Saldo da Dotação	Nome do Recurso
	33904004	COMUNICAÇÃO DE DADOS	02.01.00.04.122.0003.2.003	GABINETE DO PREFEITO E DEPENDÊNCIAS	621	1	110.0000	260.000,00	TESOURO
	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
	33904004	COMUNICAÇÃO DE DADOS	02.02.00.04.122.0004.2.004	SEC. MUN. DE ADMINISTRAÇÃO	696	1	110.0000	80.000,00	TESOURO
	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
	33904004	COMUNICAÇÃO DE DADOS	02.02.00.04.124.0004.2.013	MANUTENÇÃO DO CONTROLE INTERNO	729	1	110.0000	11.000,00	TESOURO
	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
	33904004	COMUNICAÇÃO DE DADOS	02.03.00.04.122.0006.2.008	SEC. MUN. DE PLANEJAMENTO	2404	1	110.000	12.000,00	TESOURO
	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
	33904004	COMUNICAÇÃO DE DADOS	02.04.00.12.361.0014.2.014	SEC. MUN. DE EDUCAÇÃO E CULTURA - ENSINO FUNDAMENTAL	2445	1	2200000	110.000,00	TESOURO
	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
	33904004	COMUNICAÇÃO DE DADOS	02.04.00.12.365.0016.2.016	MANUT. ENSINO INFANTIL - PRÉ-ESCOLA	2446	1	213.0000	70.000,00	TESOURO
	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
	33904004	COMUNICAÇÃO DE DADOS	02.04.00.13.391.0027.2.049	MANUT. DO PATRIMÔNIO HISTÓRICO, ARTÍSTICO E ARQUEOLÓGICO	2447	1	110.0000	7.000,00	TESOURO
	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							

PARECER
Examinado e aprovado pela Secretaria Mun.dos
Negócios Juridicos de acordo com a Lei 8.666/93
Atualizada pela Lei 8.883/94
Bastos-SP, 23 de outubro de 2019
Rafael Teixeira Sebastiani – OAB/SP 355751
Procurador Jurídico

	33904004	COMUNICAÇÃO DE DADOS	02.05.00.10 .122.0047.2 .074	MANUT. DA SEC. DE SAÚDE	716	1	310.0000	120.000,00	TESOURO
	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
	33904004	COMUNICAÇÃO DE DADOS	02.05.00.10 .301.0037.2 .017	MANUT. DO FUNDO MUN. DE SAÚDE	820	1	310.0000	80.000,00	TESOURO
	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
	33904004	COMUNICAÇÃO DE DADOS	02.05.00.10 .301.0037.2 .017	MANUT. DO FUNDO MUN. DE SAÚDE	821	5	300.0001	20.000,00	PAB
	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
	33904004	COMUNICAÇÃO DE DADOS	02.05.00.10 .301.0037.2 .017	MANUT. DO FUNDO MUN. DE SAÚDE	1915	2	300.0056	48.000,00	PAB
	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
	33904004	COMUNICAÇÃO DE DADOS	02.05.00.10 .301.0037.2 .057	MANUT. DO PROGRAMA SAÚDE DA FAMÍLIA - PSF	822	1	310.000	20.000,00	TESOURO
	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
	33904004	COMUNICAÇÃO DE DADOS	02.05.00.10 .301.0037.2 .103	MANUTENÇÃO DO CEO	823	1	310.0000	10.000,00	TESOURO
	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
	33904004	COMUNICAÇÃO DE DADOS	02.05.00.10 .302.0017.2 .120	PRONTO-SOCORRO MUNICIPAL	724	1	310.0000	20.000,00	TESOURO
	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
	33904004	COMUNICAÇÃO DE DADOS	02.05.00.10 .302.0038.2 .067	TETO ATENÇÃO HOSPITALAR E AMBULATORIAL	827	1	310.0000	10.000,00	TESOURO
	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
	33904004	COMUNICAÇÃO DE DADOS	02.05.00.10 .302.0038.2 .142	MANUT. DA REDE DE SAÚDE MENTAL	826	1	310.0000	10.000,00	TESOURO
	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
	33904004	COMUNICAÇÃO DE DADOS	02.05.00.10 .304.0032.2 .068	MANUT. DA VIGILÂNCIA SANITÁRIA	828	1	310.000	10.000,00	TESOURO
	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							

PARECER
Examinado e aprovado pela Secretaria Mun.dos
Negócios Juridicos de acordo com a Lei 8.666/93
Atualizada pela Lei 8.883/94
Bastos-SP, 23 de outubro de 2019
Rafael Teixeira Sebastiani – OAB/SP 355751
Procurador Jurídico

	33904004	COMUNICAÇÃO DE DADOS	02.05.00.10 .305.0032.2 .018	MANUT. DA VIGILÂNCIA EPIDEMIOLÓGICA	829	1	310.0000	10.000,00	TESOURO
	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
	33904004	COMUNICAÇÃO DE DADOS	02.06.00.27 .812.0019.2 .019	MANUT. DA SEC. MUN. DE ESPORTES	697	1	110.000	10.000,00	TESOURO
	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
	33904004	COMUNICAÇÃO DE DADOS	02.07.00.04 .122.0004.2 .020	MANUT. SEC. MUN. DOS NEGÓCIOS JURÍDICOS	1950	1	110.0000	5.000,00	TESOURO
	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
	33904004	COMUNICAÇÃO DE DADOS	02.08.00.08 .244.0021.2 .021	MANUT. SEC. DE PROMOÇÃO SOCIAL	698	1	510.0000	40.000,00	TESOURO
	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
	33904004	COMUNICAÇÃO DE DADOS	02.09.00.20 .606.0026.2 .026	MANUT. DA SEC. DE AGRICULTURA E MEIO AMBIENTE	717	1	110.0000	10.000,00	TESOURO
	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
	33904004	COMUNICAÇÃO DE DADOS	02.11.00.08 .243.0024.2 .025	MANUT. DO FUNDO MUN. DOS DIRETOS DA CRIANÇA E DO ADOLESCENTE	719	1	500.0003	8.000,00	TESOURO
	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
	33904004	COMUNICAÇÃO DE DADOS	02.12.00.23 .695.0030.2 .053	MANUT. DA SEC. DE TURISMO	718	1	110.0000	20.000,00	TESOURO
	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
	33904004	COMUNICAÇÃO DE DADOS	02.13.00.04 .122.0004.2 .082	MANUT. DA SEC. DE FINANÇAS	836	1	110.0000	95.000,00	TESOURO
	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
2020								**1.096.000,00**	

Neusa Kyoka Hitaka Nishida

Assessora Div. Contabilidade

R.G. 18.913.743-5 SSP/SP

14 - DAS SANÇÕES PARA O CASO DE INADIMPLEMENTO

PARECER
Examinado e aprovado pela Secretaria Mun.dos
Negócios Juridicos de acordo com a Lei 8.666/93
Atualizada pela Lei 8.883/94
Bastos-SP, 23 de outubro de 2019
Rafael Teixeira Sebastiani – OAB/SP 355751
Procurador Jurídico

14.1 - Ficará impedida de licitar com a Administração direta pelo prazo de até 5 (cinco) anos, ou enquanto perdurarem os motivos determinantes da punição, a pessoa física ou jurídica, que praticar quaisquer atos previstos no artigo 7º da Lei Federal nº 10.520, de 17 de julho de 2002.

14.2 - A sanção de que trata o subitem anterior poderá ser aplicada subsidiariamente as disposições da Lei Federal n. 8.666/93 e alterações posteriores, garantido o exercício da prévia e ampla defesa e registrada no Cadastro de fornecedores.

15 - DAS DISPOSIÇÕES FINAIS

15.1 - As normas disciplinadoras desta licitação serão interpretadas em favor da ampliação da disputa, respeitada a igualdade de oportunidade entre as licitantes e desde que não comprometam o interesse público, a finalidade e a segurança da contratação.

15.2 - O resultado do presente certame será divulgado no D.O.E (Diário Oficial do Estado).

Os demais atos pertinentes a esta licitação, passíveis de divulgação, serão publicados no Diário Oficial do Estado.

15.3 - Os envelopes contendo os documentos de habilitação das demais licitantes ficarão à disposição para retirada mediante protocolo, na Divisão de Compras e Licitações da Prefeitura Municipal, pelo prazo de 30 (trinta) dias após a entrega, ultrapassado este prazo sem a retirada dos documentos, os mesmos serão incinerados.

15.4 - Até 2 (dois) dias úteis anteriores à data fixada para o recebimento das propostas, qualquer pessoa poderá solicitar esclarecimentos(e-mail pmbcomp3@bastos.sp.gov.br ou protocolar no setor competente da Prefeitura), providências ou impugnar o ato convocatório do Pregão.

A petição será dirigida à autoridade subscritora do Edital que decidirá no prazo de 1 (um) dia útil.

Acolhida a petição contra o ato convocatório, será designada nova data para a realização do certame.

15.5 - Os casos omissos do presente Pregão serão solucionados pelo Pregoeiro.

Para dirimir quaisquer questões decorrentes da licitação, não resolvidas na esfera administrativa, será competente a Vara Distrital da Cidade de Bastos, com renúncia expressa a qualquer outro por mais privilegiado que seja.

PREFEITURA DO MUNICÍPIO DE BASTOS,
AOS 23 DE OUTUBRO DE 2019

MANOEL IRONIDES ROSA
PREFEITO MUNICIPAL

PARECER
Examinado e aprovado pela Secretaria Mun.dos
Negócios Juridicos de acordo com a Lei 8.666/93
Atualizada pela Lei 8.883/94
Bastos-SP, 23 de outubro de 2019
Rafael Teixeira Sebastiani – OAB/SP 355751
Procurador Jurídico

TERMO DE REFERENCIA – ANEXO I
PREGÃO PRESENCIAL Nº 98/2019

PROCESSO 141/2019

OBJETO:
CONTRATAÇÃO DE EMPRESA ESPECIALIZADA PARA PRESTAÇÃO DE SERVIÇOS DE TELECOMUNICAÇÕES E TECNOLOGIA DA INFORMAÇÃO, SENDO ELES: (1) PRESTAÇÃO DE SERVIÇO DE TELECOMUNICAÇÕES STFC (SERVIÇO TELEFÔNICO FIXO COMUTADO) NAS MODALIDADES ANALÓGICO E DIGITAL, (2) FORNECIMENTO DE LINK DEDICADO DE ACESSO À INTERNET, (3) FORNECIMENTO E IMPLANTAÇÃO DE SOLUÇÃO DE SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO, NOS TERMOS DAS CONCESSÕES OUTORGADAS PELA AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES – ANATEL, TODOS OS SERVIÇOS EM CONFORMIDADE COM AS ESPECIFICAÇÕES CONSTANTES NO ANEXO I, DE NATUREZA CONTINUADA, EM REGIME 24X7X365

JUSTIFICATIVA:

(1) Link Dedicado de internet: A Contratação de serviços de internet, justifica-se perante a necessidade de comunicação externa entre os setores, munícipes, fornecedores e demais situações que demandem troca de informações.

(2) Solução de Serviços Gerenciados de Segurança da Informação: A aquisição de solução de serviços gerenciados de segurança para o Departamento de TI desta prefeitura, justifica-se mediante a necessidade de garantir a segurança e controle das informações, que são de essenciais para desenvolvimento das atividades administravas desenvolvidas no âmbito deste Órgão, seguindo a LGPD.

(3) Serviço de Telecomunicação STFC (Serviço Telefônico Fixo Comutado): esta contratação justifica-se, mediante a necessidade de comunicação entre os servidores, com munícipes e fornecedores, e demais situações que demandem troca de informações.

ESPECIFICAÇÕES TECNICAS:

1. Dos Acessos

1.1. Linhas telefonicas

1.1.1. Fornecer linhas telefônicas analógicas nas quantidades e endereços estabelecidos na **Tabela 1.**

1.1.2. Ativar novas linhas telefônicas conforme necessidade da CONTRATANTE;

PARECER
Examinado e aprovado pela Secretaria Mun.dos
Negócios Juridicos de acordo com a Lei 8.666/93
Atualizada pela Lei 8.883/94
Bastos-SP, 23 de outubro de 2019
Rafael Teixeira Sebastiani – OAB/SP 355751
Procurador Jurídico

1.1.3. Desativar linhas telefônicas que estiverem em operação conforme necessidade da CONTRATANTE;

1.1.4. Possibilidade de serviços adicionais como identificador de chamadas, busca entre terminais, bloqueio de ligações a cobrar ou DDD, DDI e celular conforme necessidade da CONTRATANTE.

1.1.5. Novas linhas telefônicas deverão ser instaladas no prazo máximo de 10 dias;

1.1.6. Devem ser telealimentadas, afim de garantir a comunicação mesmo na falta de energia elétrica.

1.1.7. Tecnologias alternativas como FWT (Fixed wireless Terminal) serão permitidas somente para endereços onde não houver disponibilidade de par metálico.

1.1.8. Central de Atendimento 24h por dias, 365 dias por ano através de um número 0800;

1.1.9. A CONTRATADA deverá manter a mesma numeração atualmente utilizada (números de telefone) conforme critérios da Portabilidade regulamentada pela ANATEL, para os números relacionados no Anexo I, além de outros que tiverem sua inclusão neste certame.

1.1.10. Nos casos onde não for possível a instalação por par metálico ou FWT, que dependam de projeto de infraestrutura, deverá ser apresentado para a CONTRATANTE que será responsável pelo custo do projeto.

1.2. Tronco Digital E1

1.2.1. Fornecer tronco digital E1 e faixas DDR nas quantidades estabelecidas no **Anexo II – Tabela 2;**

1.2.2. Interface tipo G.703

1.2.3. Sinalização de Linha tipo R2D

1.2.4. Sinalização de Registro tipo MFC 5C ou 5S

1.2.5. Ativar e desativar troncos conforme necessidade da CONTRATANTE e segundo o limite estabelecido na lei 8.666;

1.2.6. Prazo de instalação de 90 dias;

1.2.7. Disponibilidade mensal (SLA - Service level agreement) de 99% ao mês;

1.2.8. Início de atendimento em caso de defeito em até 4 horas

1.2.9. Meio de atendimento em par-metálico, fibra-óptica;

1.2.10. Em casos onde for constatada inviabilidade de instalação a CONTRATADA deverá encaminhar as condições de atendimento (custo, prazo e meio) para análise da CONTRATANTE e será objeto de aditivo contratual.

1.2.11. Central de Atendimento 24h por dias, 365 dias por ano através de um numero 0800;

1.2.12. Mudança de endereço de acessos instalados tem o mesmo prazo de instalação de novos acessos;

1.2.13. A CONTRATADA deverá manter a mesma numeração atualmente utilizada (números de telefone) conforme critérios da Portabilidade regulamentada pela ANATEL, para os números relacionados no **Anexo II – Tabela 2**, além de outros que tiverem sua inclusão neste certame.

2. Do tráfego Telefônico

2.1. Método

2.1.1. Conforme especificações mínimas estabelecidas pelo órgão regulador;

2.1.2. Informar os custos de assinatura individuais das linhas telefonicas, troncos digitais , faixas DDR e serviço 0800;

2.1.3. A tarifação das chamadas deverá ser realizada em minutos;

2.1.4. As tarifas utilizadas deverão ter como base aqueles constantes do Plano básico de serviços ou do Plano alternativo de serviços, regulamentado para o setor de telecomunicação e informado através do preenchimento da Proposta Comercial**,** com todos os impostos regulamentados e descontos concedidos a critério da Licitante;

2.1.5. As mensalidades para as linhas analógicas deverão contemplar os custos de 150 (cento e cinquenta) minutos para ligação local fixo-fixo (inclusos nesta cotação);

2.2. Perfil de tráfego

2.2.1. Deverão ser considerados os volumes de chamadas indicadas no **Anexo** como referência orientativa para apresentação de proposta;

2.2.2. O Perfil de Tráfego e seus custos **(Anexo III)**, compõe-se de uma ESTIMATIVA, em minutos e em valores, baseadas nas faturas das contas telefônicas da CONTRATANTE relativa às chamadas originadas em seu âmbito, bem como outros serviços atualmente utilizados;

2.2.3. O Perfil de Tráfego do **Anexo III**, servirá tão somente de subsídio para análise da proposta global mais vantajosa e portanto, não implicam em qualquer compromisso futuro ou restrição quantitativa de uso para a CONTRATANTE.

2.3. Da fatura

2.3.1. As faturas de cada serviço devem ser encaminhadas via papel, individualizada por linha seja analógica ou digital, com valor total e o respectivo descritivo com os valores das ligações;

2.4. Responsabilidades da contratante

Toda a infra-estrutura civil, elétrica, ar condicionado, leitos de passagem de cabos, rede interna (cabeamento horizontal) e serviços são de responsabilidade da contratante, incluindo a adequação

conforme as necessidades de implantação do projeto, bem como disponibilizar o PABX com interface para E1 30 canais

Da mesma forma, será de responsabilidade do CONTRATANTE reparar ou refazer os acabamentos necessários para instalação do objeto pela CONTRATADA.

2.4.1. Requisitos mínimos sugeridos

2.4.1.1. Circuito Bifásico 220 / 110V (suportado por no-break, com disjuntor de proteção 50 A) .

2.4.1.2. Rede estabilizada, ininterrupta, suportada por gerador, para garantir perfeito funcionamento dos equipamentos;

2.4.1.3. Infra-estrutura para que o acessos digitais (E1) ou analógicos (linhas telefônicas) cheguem até os equipamentos PABX fornecidos;

2.4.1.4. Quadro de Força com circuitos independentes e exclusivos para os equipamentos com disjuntores de 110 e 220V;

2.4.1.5. Cabeamento vertical e horizontal para a ativação dos ramais;

2.4.1.6. Jumpeamento do Bloco PABX para rede cliente;

2.4.1.7. Disponibilizar local preparado para acomodar o PABX e seus periféricos;

2.4.1.8. Aterramento < 10 ohms bitola 16 mm, conforme norma NBR 5410 de 1997da ABNT em ponto único para equalização de potencial, conforme norma vigente - NBR5410/NB - 3 - 1997;

2.4.1.9. Piso e paredes com acabamento final e vedação contra pó e umidade;

2.4.1.10. Extintor de incêndio obedecendo às normas do corpo de bombeiros;

2.4.1.11. Ambiente com climatização adequada, boa iluminação e acesso restrito;

2.4.2. Prazo e condições de instalação

2.4.2.1. O escopo de instalação está restrito a ativação e teste dos equipamentos fornecidos, toda a infra-estrutura necessária e quaisquer programações diferenciadas para interligação de sistemas, são de responsabilidade do CONTRATANTE;

2.4.2.2. O prazo de instalação é de 30 (trinta) dias após assinatura do contrato, prorrogáveis por mais 30 (trinta) dias, à critério da Administração;

2.4.3. Condições de manutenção

Os serviços especializados na rede interna: manutenção, configuração e ampliação são de responsabilidade do CONTRATANTE;

3.3– LOCAL, PRAZO E CONDIÇÕES DE ENTREGA:

3.3.1 - A habilitação das linhas e o consequente início da prestação dos serviços contratados deverão ocorrer no prazo máximo de 30 (trinta) dias corridos, podendo ser prorrogados por mais 15 dias

mediante justificativa, contados a partir da data de entrega dos Chips e caso a Prefeitura solicite a portabilidade das linhas o prazo será o mínimo previsto pela ANATEL.

3.4- DO PRAZO DE VIGÊNCIA DO CONTRATO

3.4.1– O contrato terá vigência por doze (12) meses, iniciando-se a partir de sua assinatura, podendo ser prorrogado a critério da Prefeitura Municipal de Borborema com fulcro no artigo 57, inciso II, da Lei nº 8.666/93 e legislações posteriores.

Link dedicado de Dados (internet)

Link dedicado de dados (Internet) com velocidade informada no Anexo III, com as seguintes especificações mínimas:

– Acesso:

– O link deverá ser fornecido obrigatoriamente através de fibra óptica;

– Deverá ser bidirecional e simétrico na velocidade mínima de 30 Mbps;

– O uso de Fibra Óptica como meio físico de transporte dos dados deverá ser utilizado em todos os enlaces (trajeto) desde o backbone da operadora de telecomunicações, até o roteador instalado dentro do datacenter da CONTRATANTE;

– Velocidade mínima de 96,8% da velocidade nominal, tanto para download como para upload;

– Disponibilidade real mínima de 99,2% (SLA);

– A CONTRATANTE não terá qualquer tipo de limitação quanto a quantidade (em bytes) e conteúdo da informação trafegada no acesso;

– Possuir taxa de perda de pacotes menor ou igual a 1%;

– Latência média de no máximo 220 ms;

– Fornecimento mínimo de 6 endereços IP (V4) para cada link;

– A CONTRATADA deverá possuir Termo de Autorização para a prestação de Serviço Comunicação Multimídia (SCM) outorgado pela ANATEL;

– A CONTRATADA deverá possuir central de atendimento 24 horas por dia, 365 dias por ano, através de um número 0800;

– Em caso de defeito, o início do atendimento deverá ser de no máximo 4 horas;

– O Acesso deve ser realizado sem necessidade de provedor;

– Painel web ou software disponibilizado pela CONTRATADA, para acompanhamento, gerenciamento dos links de dados, tais como, criação de relatórios de métricas de uso de dados, métricas de tempo de reparo, etc.

– Saída para backbone internacional própria;

– Saída internacional agregada maior ou igual a 5 Gbps;

– Latência média menor ou igual à 75 ms;
– Perda de pacotes menor ou igual a 1%;
– Disponibilidade mensal do backbone internacional maior ou igual à 99,7%;

– Dos equipamentos (roteadores).
– O roteador será fornecido pela CONTRATADA, com instalação, configuração e gerencia;
– A configuração será executada para que a rede de computadores da contratante possua acesso a internet;
– Possuir quantidade mínima de memória que atenda a velocidade funcionalidades deste item, em conformidade com as recomendações do fabricante;
– Possuir protocolo de gerenciamento SNMP;
– Todos os roteadores deverão ter capacidade para suportar tráfego com banda completamente ocupada, sem exceder a 80% de utilização de CPU e memória;
– Responder por todas as normas definidas pela Agencia Nacional de Telecomunicações – ANATEL;

2. – Prazo e condições de instalação.
2.1 – O escopo de instalação esta restrito a ativação e teste dos equipamentos fornecidos, toda a infraestrutura necessária e quaisquer programações diferenciadas para interligação de sistemas, são de responsabilidade da CONTRATANTE;
2.2 – O prazo máximo de instalação é de 90 (noventa) dias após assinatura do contrato, podendo ser prorrogado por mais 30 dias;

SERVIÇO GERENCIADO DE SEGURANÇA

Contratação de empresa especializada para fornecimento de MSS (*Managed Security Services*) sobre a solução de segurança com as funcionalidades descritas em **ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO**, contemplando serviços de instalação, configuração, manutenção, suporte técnico remoto, monitoramento e gerenciamento na modalidade 24x7x365, pelo período de 36 meses.

1 DESCRIÇÃO DO SERVIÇO

1.1. Solução de Gerenciamento com fornecimento de hardware e software

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

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

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

1.2. Gerenciamento/Manutenção

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

1.3. Serviço de comunicação de dados

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

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

1.4. Infraestrutura mínima necessária.

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

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

1.4.3. Responsabilidades do SOC

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

1.4.3.1.1. Segurança física: mecanismos de monitoração e registro de todo e qualquer acesso ao SOC, utilizando-se de câmeras de segurança;

1.4.3.1.2. Acesso ao SOC controlado por mecanismos de autenticação forte (pelo menos autenticação de dois fatores); ambiente isolado de outros que não sejam destinados à operacionalização e controle de segurança;

1.4.3.1.3. Mecanismos de prevenção, detecção e combate a incêndios;

1.4.3.1.4. Política de acesso lógico: possuir autenticação forte no acesso aos equipamentos que estarão nas dependências da **CONTRATANTE**, com usuários segregados por função e registros para controle de auditoria;

1.4.3.1.5. Possuir políticas definidas para criação, exclusão e manutenção de chaves, senhas e perfis de acesso.

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

1.4.4.1. <u>MANUTENÇÃO</u>

1.4.4.1.1. Fornecer apoio técnico necessário para realizar o diagnóstico de eventos de falha em seus ativos de segurança. Através da análise dos logs do equipamento, o SOC deverá determinar se houve alguma avaria em um dos componentes de hardware da solução e identificar a necessidade ou não de sua substituição.

1.4.4.1.2. Efetuar o processo de RMA (sigla em inglês de *return merchandise authorization*).

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

1.4.4.2. <u>SUPERVISÃO</u>

1.4.4.2.1. Efetuar a monitoração constante da capacidade e da disponibilidade da infraestrutura de segurança contratada.

1.4.4.2.2. Compreender as atuais demandas sobre os recursos de segurança e criar previsões para futuras solicitações quando necessário.

1.4.4.2.3. Avaliar se o nível de disponibilidade é sustentável, permitindo o negócio atingir seus objetivos de forma consistente.

1.4.4.2.4. Ter uma arquitetura de monitoração, baseada em solução que utiliza o protocolo SNMP para realizar os *healthchecks*.

1.4.4.2.5. Processar e disponibilizar em relatórios mensais os dados coletados.

1.4.4.2.6. Identificar que o componente atingiu certo nível de utilização (threshold).

1.4.4.2.7. Alertar e encaminhar para os técnicos responsáveis pela administração.

1.4.4.2.8. Acompanhar a saúde dos dispositivos supervisionando-os 24x7.

1.4.4.2.9. Comunicar ao **CONTRATANTE**, anomalias quando um componente monitorado apresentar índices não usuais.

1.4.4.2.10. Prover a monitorização da saúde dos dispositivos

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

1.4.4.3. ADMINISTRAÇÃO

1.4.4.3.1. Realizar a operação remota, gestão de mudança e gestão de configuração dos dispositivos de segurança contratado.

1.4.4.3.2. Resolução nos incidentes de segurança que ocorrem nos elementos administrado (s), detectados pelo monitoramento ou que sejam informados pela **CONTRATANTE**.

1.4.4.3.3. Planejar e realizar implementação de mudanças no ambiente contratado e gerenciado, sejam elas solicitadas pelo **CONTRATANTE** ou mesmo por recomendação da própria **CONTRATADA**, baseados nas melhores práticas de gestão.

1.4.4.3.4. Efetuar tarefas operacionais básicas, tais como executar *backup/restore* de configurações e gerenciamento do ambiente contratado.

1.4.4.3.5. Garantir o correto funcionamento dos dispositivos administrados.

1.4.4.3.6. Manter e atualizar o ambiente contratado com o software do dispositivo na versão mais atual recomendada pelo fabricante.

1.4.4.3.7. Efetuar aplicação de patches para a resolução de incidentes, correção de vulnerabilidades e prevenção de incidentes de segurança.

1.4.4.3.8. Efetuar atualização de software e patches somente se e quando autorizada pela **CONTRATANTE**, através do processo de gestão da mudança.

1.4.4.3.9. Informar ao **CONTRATANTE** dos possíveis riscos de segurança identificados através da administração da infraestrutura ou através das ferramentas de administração.

1.4.4.3.10. Atender as dúvidas e solicitações de segurança da **CONTRATANTE**.

1.4.4.3.11. Acompanhar e encaminhar os chamados através de ferramenta.

1.5. Implantação da Solução:

1.5.1. A implantação da solução de hardware e software deverá ser realizada no prazo de até 120 (cento e vinte dias) dias da contratação, mediante entrega de cronograma, detalhando as fases do projeto de implantação. Esse cronograma deverá ser aprovado pelo **CONTRATANTE**, sendo a implantação iniciada somente após esta aprovação.

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

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

1.5.2.2. Implantação: Relatório de implantação;

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

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

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

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

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

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

2. PRESTAÇÃO DOS SERVIÇOS

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

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

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

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

2.2.1.2. Definir as estratégias, políticas e regras a serem implantadas, e analisar/aprovar as solicitações;

2.2.1.3. Tomar as providências necessárias, em caso da ocorrência de algum incidente (análise dos logs, rastreamento da ocorrência).

2.2.2. A **CONTRATANTE** poderá realizar inspeção nas instalações do SOC, com o objetivo de verificar a segurança física e lógica do ambiente, a qualquer tempo com a **CONTRATADA**.

2.3. Ocorrência de Incidentes

2.3.1. No caso de detecção de algum incidente de segurança, a **CONTRATADA** deverá notificar a **CONTRATANTE** dentro do período estabelecido no SLA, para que sejam tomadas as medidas corretivas e legais necessárias.

2.3.1.1. São considerados incidentes de segurança: os acessos indevidos, instalação de códigos maliciosos, ataques por força bruta, ou qualquer outra ação que vise prejudicar a funcionalidade ou a disponibilidade dos serviços da **CONTRATANTE**.

2.3.2. A **CONTRATADA** comunicará imediatamente a **CONTRATANTE**, para que possam ser tomadas ações preventivas, nos casos de tentativas, sem sucesso, de acessos indevidos, de instalação de códigos maliciosos, ou de qualquer outra ação que venha pôr em risco a segurança do ambiente do **CONTRATANTE**, em que seja evidenciada a insistência, por parte da pessoa mal-intencionada.

2.3.3. A **CONTRATADA** disponibilizará todas as informações necessárias (origem do ataque, tipo de ataque, data e hora, logs, etc.) para que sejam apurados os incidentes de segurança reportados junto ao ambiente contratado.

2.4. Encerramento dos Serviços de Monitoração Remota da Segurança

2.4.1. Quando do encerramento da prestação do serviço de monitoração remota da segurança, a **CONTRATADA** retirará os componentes da solução.

2.4.2. Todas as informações de customização, políticas e regras, logs de auditoria serão disponibilizadas para a **CONTRATANTE** e, em seguida, eliminadas da base de dados da **CONTRATADA**.

2.5. Confidencialidade da Informação.

2.5.1. Todas as informações que trafegam nos equipamentos, bem como todas e quaisquer informações originadas pela **CONTRATANTE**, que a **CONTRATADA** venha a ter acesso serão consideradas “Informações Confidenciais”.

2.5.2. A **CONTRATADA** se compromete a guardar confidencialidade e a não utilizar qualquer tipo de Informação Confidencial para propósitos estranhos àqueles definidos neste Termo de Referência ou em benefício próprio ou de terceiros.

2.5.3. A **CONTRATADA** se compromete a adotar as medidas necessárias para que seus dirigentes, empregados, e em geral todas as pessoas que trabalham sob sua responsabilidade, que precisem conhecer a Informação Confidencial, mantenham a confidencialidade acordada neste instrumento, sendo responsável pela ruptura do compromisso de confidencialidade pelos seus empregados.

2.5.4. A **CONTRATADA** se obriga a devolver ou destruir imediatamente todo o material que contenha Informações Confidenciais, tão logo ocorra a rescisão ou término da vigência do contrato firmado entre as partes.

2.5.5. A **CONTRATANTE** também se compromete a tratar como confidenciais todas as informações de propriedade da **CONTRATADA**, que vier a ter conhecimento, durante a vigência do contrato.

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

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

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

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

3.1.2. Abaixo os tempos de atendimento:

Serviço	Definição	Crítico	Alto	Médio	Baixo

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

3.1.3. SLO de Solicitações e Consultas:

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

ESPECIFICAÇÕES TECNICAS DA SOLUÇÃO

SOLUÇÃO DE SEGURANÇA DE REDE

Solução 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, sendo fornecida em hardware específico.

O hardware e o software fornecidos não podem constar, no momento da apresentação da proposta, em listas de *end-of-sale, end-of-support, end-of-engineering-support* ou *end-of-life* do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante.

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

Item	Descrição	Quantidade
HARDWARE DE FIREWALL		
1	Cluster de Firewall **UTM/NGFW**	1 unidade
SOFTWARE FIREWALL		
2	Pacote de licenças de NG Firewall, IPS/IDS, Controle de Aplicação, Filtro de URL, Anti-vírus, Anti-Malware.	1 unidade

1. ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO

1.1. A performance de todos os serviços ativos de Threat Prevention, deverá ser de 1.5Gbps ou superior.

1.2. Performance de Inspeção de tráfego criptografado (SSL) de no mínimo 290 Mbps, o throughput devem ser comprovados por documento de domínio público do fabricante.

1.3. Performance de IPS de 1.4Gbps ou superior;

1.4. Suporte a, no mínimo, 1.000.000 de conexões do tipo SPI simultâneas;

1.5. Suporte a, no mínimo, 14.000 novas conexões por segundo;

1.6. Disco interno SSD para armazenamento de no mínimo 16 Gb;

1.7. Deve suportar fonte de alimentação interna redundante com chaveamento automático de 100-240 VAC;

1.8. Deverá possuir 4 interfaces de 1GbE SFP;

1.9. 12 interfaces de rede 10/100/1000 base-TX. Todas as interfaces devem possuir mecanismo de auto-sense e seleção de modo half/full duplex.

1.10. As interfaces devem suportar as seguintes atrubuições:

1.10.1. Segmento Wan ou externo;

1.10.2. Segmento WAN, secundário com possibilidade de ativação de recurso para redundância de WAN com balanceamento de carga e WAN Failover por aplicação. O equipamento deverá suportar no mínimo balanceamento de 4 links utilizando diferentes métricas pré-definidas pelo sistema e configuráveis pelo administrador.

1.10.3. Segmento LAN ou rede interna.

1.10.4. Segmento LAN ou rede interna podendo ser configurado como DMZ (Zona desmilitarizada)

1.10.5. Segmento LAN ou rede interna ou Porta de sincronismo para funcionamento em alta disponibilidade

1.10.6. Segmento ou Zona exclusiva para controle de dispositivos Wireless dedicado, com controle e configuração destes dispositivos.

1.10.7. 01 (uma) interface do tipo console ou similar;

1.10.8. 01 (uma) interface de rede dedicada para gerenciamento;

1.11. A VPN Client-to-Site IPsec deve ser licenciada para, no mínimo, 50 usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para no mínimo, 1000 usuários simultâneos, com aquisição de licença futura;

1.12. A VPN SSL deve ser licenciada para, no mínimo, 2 usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para no mínimo, 500 usuários simultâneos, com aquisição de licença futura;

1.13. Suportar 1000 túneis de VPN IPSEC simultâneos;

1.14. Suportar, no mínimo, 1.4Gbps de throughput de VPN IPSEC

1.15. Em appliance com no máximo 2U de altura, com kit de montagem em rack de 19".

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

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

1.18. 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

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

1.20. Possuir redundância do sistema de refrigeração do produto (ventoinha).

2. CARACTERÍSTICAS GERAIS PARA SOLUÇÃO DE FIREWALL

2.1. Todas as funcionalidades descritas devem funcionar no mesmo appliance sem a necessidade de composição de um ou mais produtos;

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

2.3. O hardware e software que executem as funcionalidades de proteção de rede devem ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;

2.4. O equipamento deverá ser baseado em hardware desenvolvido com está finalidade, ou seja, não sendo aceita soluções baseadas em plataforma PC ou equivalente;

2.5. Não serão permitidas soluções baseadas em sistemas operacionais abertos (OpenSource) como Free BSD, Debian ou mesmo Linux;

2.6. Todo o ambiente deverá ser gerenciado através de uma única interface sem a necessidade de produtos de terceiros para compor a solução;

2.7. Deve ser possível suportar arquitetura de armazenamento de logs redundante, permitindo a configuração de equipamentos distintos;

2.8. A solução deverá suportar monitoramento através de SNMP v2 e v3;

2.9. Deve oferecer as funcionalidades de backup/restore tanto da configuração quanto do firmware/sistema operacional através da interface gráfica, assim como permitir ao administrador agendar procedimentos de backups da configuração em determinado dia e hora. O appliance deve armazenar no mínimo 02 (duas) versões distintas do sistema operacional, sendo possível escolher qual versão será inicalizada;de backups da configuração em determinado dia e hora;

2.10. Deve oferecer a funcionalidade de seleção da velocidade da "Porta" a ser realizada preferencialmente através da interface gráfica de gerenciamento. As interfaces devem suportar obrigatoriamente as seguintes atribuições:

- Segmento WAN, ou externo.
- Segmento WAN, secundário com possibilidade de ativação de recurso para redundância de WAN com balanceamento de carga e WAN Failover por aplicação. O equipamento deverá suportar no mínimo balanceamento de 4 links utilizando diferentes métricas pré-definidas pelo sistema e configuráveis pelo administrador.
- Segmento LAN ou rede interna.
- Segmento LAN ou rede interna podendo ser configurado como DMZ (Zona desmilitarizada)
- Segmento LAN ou rede interna ou Porta de sincronismo para funcionamento em alta disponibilidade
- Segmento ou Zona exclusiva para controle de dispositivos Wireless dedicado, com controle e configuração destes dispositivos.

2.11. Suporte a definição de VLAN no firewall, conforme padrão IEEE 802.1q e ser possível criar sub-interfaces lógicas associadas a VLANs e estabelecer regras de filtragem (Stateful Firewall) entre elas;

2.12. A solução deve suportar configuração de link-aggregation de interfaces suportando o protocolo 802.3ad para aumento de throughput.

2.13. A solução deve suportar configuração de port-redundacy de interfaces para a alta disponibilidade de interfaces;

2.14. Os dispositivos de proteção devem ter a capacidade de operar de forma simultânea mediante o uso de suas interfaces físicas nos seguintes modos:

2.15. Modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3);

2.16. Modo sniffer, para inspeção via porta espelhada do tráfego de dados da rede;

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

2.18. 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;

2.19. Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas.

2.20. Possuir DHCP Server interno;

2.21. Suporte a encaminhamento de pacotes UDPs multicast/broadcast entre diferentes interfaces e zonas de segurança como como DHCP Relay, suportando os protocolos e portas:

- Time service—UDP porta 37
- DNS—UDP porta 53
- DHCP—UDP portas 67 e 68
- Net-Bios DNS—UDP porta 137
- Net-Bios Datagram—UDP porta 138
- Wake On LAN—UDP porta 7 e 9
- mDNS—UDP porta 5353
- Suporte a Jumbo Frames;
- Implementar sub-interfaces ethernet lógicas;
- Deve suportar os seguintes tipos de NAT:
- Nat dinâmico (Many-to-1);
- Nat dinâmico (Many-to-Many);
- Nat estático (1-to-1);
- NAT estático (Many-to-Many);
- Nat estático bidirecional 1-to-1;
- Tradução de porta (PAT);
- NAT de origem;
- NAT de destino;

2.22. Suportar NAT de origem e NAT de destino simultaneamente;

2.23. Prover mecanismo contra ataques de falsificação de endereços (IP Spoofing);

2.24. Implementar mecanismo de sincronismo de horário através do protocolo NTP. Para tanto o appliance deve realizar a pesquisa em pelo menos 03 servidores NTP distintos, com a configuração do tempo do intervalo de pesquisa;

2.25. Possuir gerenciamento de tráfego de entrada ou saida, por serviços, endereços IP e regra de firewall, permitindo definir banda mínima garantida e máxima permitida em porcentagem (%) para cada regra definida;

2.26. Implementar 802.1p e classe de serviços CoS (Class of Service) de DSCP (Differentiated Services Code Points);

2.27. Permitir remarcação de pacotes utilizando TOS e/ou DSCP;

2.28. Suporte a policy based routing (PBR), com a capacidade de roteamento por endereço de origem, endereço de destino, serviço, interface ou todas as opções simultâneas;

2.29. Suportar protocolos de roteamento RIP, RIPng, OSPF, OSPFv3 e BGP;

2.30. Suportar Equal Cost Multi-Path (ECMP);

2.31. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);

2.32. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3, RIPng);

2.33. A solução deve suportar integralmente o padrão IPv6, assim como criação de regras com objetos que utilizem endereços IPv4 e IPv6;

2.34. Deve suportar no mínimo as seguintes funcionalidades ou protocolos para o padrão de endereçamento IPv6: Tunel 6 to 4, regras de acesso, objetos de enderço, limitador de conexões IPv6, monitor de conexões, DHCP, gerenciamento HTTPS via IPv6, NAT IPv6, proteção contra ataques to tipo IP Spoofing para IPv6, captura de pacotes IPv6, interface VLAN com endereço IPv6, VPN SSL com o uso do IPv6, controle de URL, Anti-Malware e anti-virus, controle de aplicação, IPS, IKEv2, ICMP6, SNMP, alta disponibilidade, RFC 1981 Path MTU Discovery for IPv6, RFC 2460 IPv6 specification, RFC 2464 Transmission of IPv6 Packets over Ethernet Networks;

2.35. Possui suporte a log via syslog;

2.36. Possuir mecanismo para possibilitar a aplicação de correções e atualizações para o firewall remotamente através da interface gráfica;

2.37. Permitir a visualização em tempo real de todas as conexões TCP e sessões UDP que se encontrem ativas através do firewall;

2.38. Permitir a geração de gráficos em tempo real, representando os serviços mais utilizados e as máquinas mais acessadas em um dado momento;

2.39. Permitir a visualização de estatísticas do uso de CPU do appliance o através da interface gráfica remota em tempo real;

2.40. A solução deverá suportar a tecnologia de SD-WAN e deverá ter no mínimo as seguintes funcionalidades:

- Capacidade de criar um overlay virtual de roteamento, de forma agnóstica a infraestrutura de rede já existente, com a combinação de quaisquer tipos de circuitos WAN;
- Capacidade de agregar no mínimo 3 (três) circuitos WAN distintos em um único canal lógico;
- Implementar segurança fim-a-fim usando solução de criptografia que de maneira automática forneça proteção à redes WANs privadas que transitam por redes públicas compartilhadas;
- Suportar e implementar QoS com classificação, marcação e priorização de tráfego com base em endereço IP de origem/destino, portas TCP/UDP de origem e destino, DSCP (Differentiated Services Code Point), tipo de aplicação camada 7 e traffic shaping nas interfaces;
- Capacidade de realizar a saída local de internet para alguns tráfegos selecionados a partir, no mínimo, dos parâmetros de IP, porta e URL;
- Controle de caminho automático baseado em políticas, com habilidade de selecionar o caminho, no mínimo, através dos seguintes parâmetros simultâneos ou não:
    - ✓ tipo de aplicação;
    - ✓ prioridade de negócio;
    - ✓ latência;
    - ✓ jitter;
    - ✓ perda de pacotes;

- ✓ A comutação dos caminhos deve ocorrer de maneira dinâmica e automática baseada nas políticas previamente aplicadas;
- ✓ Permitir a alteração da política de encaminhamento sem impacto no tráfego;
- ✓ Implementar tecnologia de reconhecimento de aplicações conhecidas (DPI), como Office 365, Facebook e Youtube, como também subaplicações associadas como Facebook Messenger e Office 365 Outlook.

ALTA DISPONIBILIDADE

2.41. A solução deve ser entregue operando em alta disponibilidade no modo Ativo/Standby, com as implementações de Failover;

2.42. Não serão permitidas soluções de cluster (HA) que façam com que o equipamento (s) reinicie após qualquer modificação de parâmetro/configuração seja realizada pelo administrador;

2.43. A solução deve ter capacidade de fazer monitoramento físico das interfaces dos membros do cluster;

2.44. A solução deve operar em alta disponibilidade implementando monitoramento logico de um host na rede, para verificar a existência de problemas lógicos na rede e possibilitar failover;

2.45. A solução deve permitir o uso de endereço MAC virtual para evitar problemas de expiração de tabela ARP em caso de Failover;

2.46. A solução deve possibilitar a sincronização de todas as configurações realizadas na caixa principal do cluster, incluindo, mas não limitado a objetos, regras, rotas, VPN´s e políticas de segurança;

2.47. A solução deve permitir visualizar no equipamento principal, o status da comunicação entre o peers do cluster, status de sincronização das configurações, status atual equipamento backup;

VPN

2.48. Criptografia 3DES, AES 128 e AES 256;

2.49. Autenticação com MD5, SHA-1, SHA-256 e SHA-384;

2.50. Diffie-Hellman: Grupo 2 (1024 bits), Grupo 5 (1536 bits) e Grupo 14 (2048 bits;

2.51. Algoritmo Internet Key Exchange (IKE);

2.52. Autenticação via certificado IKE PKI;

2.53. Deve possuir interoperabilidade com outros fabricantes de acordo com o padrão IPSEC através de RFC`s;

2.54. A solução deve suportar VPNs L2TP, incluindo suporte para iPhone, Windows phone, Android com suporte a cliente L2TP;

2.55. Solução deve suportar VPNs baseadas em políticas e VPNs baseadas em roteamento estático e dinâmico;

2.56. Suportar políticas de roteamento sobre conexões VPN IPSEC do tipo site-to-site com diferentes métricas e serviços. A rota poderá prover aos usuários diferentes caminhos redundantes sobre todas as conexões VPN IPSEC;

2.57. Solução deve incluir a capacidade de estabelecer VPNs com outros firewalls que utilizam IP públicos dinâmicos;

2.58. Permitir a definição de um gateway redundante para terminação de VPN no caso de queda do circuito primário;

2.59. Permitir que seja criado políticas de roteamentos estáticos utilizando IPs de origem, destino, serviços e a própria VPN como parte encaminhadora deste tráfego sendo este visto pela regra de roteamento, como uma interface simples de rede para encaminhamento do tráfego;

2.60. Suportar a criação de túneis IP sobre IP (IPSEC Tunnel), de modo a possibilitar que duas redes com endereço inválido possam se comunicar através da Internet;

AUTENTICAÇÃO

2.61. Permitir a utilização de LDAP, AD e RADIUS;

2.62. Permitir o cadastro manual dos usuários e grupos diretamente na interface de gerência remota do Firewall, caso onde se dispensa um autenticador remoto para o mesmo;

2.63. Suporte a uma rede com múltiplos domínios, possibilitando a integração em um ambiente onde existas domínios diferentes e totalmente segregados;

2.64. Permitir a integração com qualquer autoridade certificadora emissora de certificados X509 que seguir o padrão de PKI descrito na RFC 2459, inclusive verificando as CRLs emitidas periodicamente pelas autoridades, que devem ser obtidas automaticamente pelo firewall via protocolos HTTP e LDAP;

2.65. Permitir o controle de acesso por usuário, para plataformas Windows Me, NT, 2000, 2000, XP, Windows 7, Windows 8 e Windows 10 de forma transparente, para todos os serviços suportados, de forma que ao efetuar o logon na rede, um determinado usuário tenha seu perfil de acesso automaticamente configurado;

2.66. Permitir a restrição de atribuição de perfil de acesso à usuário ou grupo independente ao endereço IP da máquina que o usuário esteja utilizando;

2.67. Suportar recurso de autenticação única para todo o ambiente de rede, ou seja, utilizando a plataforma de autenticação atual que pode ser de LDAP ou AD; o perfil de cada usuário deverá ser obtido automaticamente através de regras no Firewall DPI (Deep Packet Inspection) sem a necessidade de uma nova autenticação como por exemplo, para os serviços de navegação a Internet atuando assim de forma toda transparente ao usuário.

Serviços como HTTP, HTTPS devem apenas consultar uma base de dados de usuários e grupos de servidores 2008/2012 com AD;

IPS

2.68. Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS integrados no próprio appliance de firewall, onde sua console de gerência deverá residir na mesma console centralizada dos appliances de segurança, com suporte a pelo menos 3.000 assinaturas;

2.69. A solução de IPS deverá possuir os seguintes mecanismos de detecção: assinaturas e trabalhar em conjunto com o controle de aplicações;

2.70. A solução de IPS deve fazer a inspeção de todo o pacote, independentemente do tamanho;

2.71. A solução de IPS deve fazer a inspeção de todo o tráfego de forma bidirecional, analisando qualquer tamanho de pacote sem degradar a performance do equipamento solicitada neste edital;

2.72. Possuir capacidade de remontagem de pacotes para identificação de ataques;

2.73. O mecanismo de inspeção deve receber e implementar em tempo real atualizações para os ataques emergentes sem a necessidade de reiniciar o appliance;

2.74. Para cada proteção de segurança, deve ser possível consultar informações no site do fabricante;

2.75. A ferramenta de log deve possuir a capacidade de criar uma regra de exceção a partir do log visualizado na gerência centralizada;

2.76. As regras de exceção devem possuir: origem, destino e serviço;

2.77. A solução deve ser capaz de inspecionar tráfego HTTPS;

2.78. Deverá possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep;

2.79. Detecção de anomalias;

2.80. A solução de IPS deve possuir política capaz de definir o modo de operação (bloqueio ou detecção);

2.81. O módulo de IPS deve possuir assinaturas voltadas para ambientes de servidores de SMTP, Web e DNS;

2.82. O mecanismo de inspeção deve receber e implementar em tempo real atualizações de novas assinaturas sem a necessidade de reiniciar o appliance;

2.83. Para cada proteção, ou para todas as proteções suportadas, deve incluir a opção de adicionar exceções baseado na origem e destino;

2.84. A solução deve ser capaz de detectar e bloquear ataques nas camadas de rede e aplicação, protegendo pelo menos os seguintes serviços: Aplicações web, serviços de e-mail, DNS, FTP, SQL Injection, ataques a sistemas operacionais e VOIP;

2.85. Deve incluir proteção contra worms;

2.86. Deve incluir uma tela de visualização situacional a fim de monitorar graficamente a quantidade de alertas de diferentes severidades e a evolução ao logo do tempo dispondo o sumario quantitativo das ameaças analisadas.

2.87. A solução deve possuir esquema de atualização de assinaturas através de um click;

2.88. Atualização de modo offline, onde poder ser baixado na base do fabricante e posteriormente fazer o upload do arquivo na solução;

2.89. A solução deve suportar importar certificados de servidor para inspeções de tráfego seguro HTTP (HTTPS) de entrada. Depois de importar esses certificados, a solução deve permitir o IPS para Inspeção segura HTTP(HTTPS);

2.90. A solução deverá ser capaz de inspecionar e proteger apenas hosts internos;

2.91. A solução deverá possuir a opção de proteções para sistemas SCADA;

2.92. Solução deverá permitir que o administrador bloqueie facilmente o tráfego de entrada e/ou saída com base em países, sem a necessidade de gerir manualmente os ranges de endereços IP dos países que deseja bloquear.

CONTROLE DE APLICAÇÃO

2.93. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades abaixo:

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

2.95. Capacidade para realizar filtragens/inspeções dentro de portas TCP conhecidas por exemplo porta 80 http, buscando por aplicações que potencialmente expõe o ambiente como: P2P, Kazaa, Morpheus, BitTorrent ou messengers;

2.96. Controlar o uso dos serviços de Instant Messengers como MSN, YAHOO, Google Talk, ICQ, de acordo com o perfil de cada usuário ou grupo de usuários, de modo a definir, para cada perfil, se ele pode ou não realizar download e/ou upload de arquivos, limitar as extensões dos arquivos que podem ser enviados/recebidos e permissões e bloqueio de sua utilização baseados em horários pré-determinados pelo administrador será obrigatório para este item.

2.97. Deverá controlar software FreeProxy tais como ToR, Ultrasurf, Freegate,etc;

2.98. Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;

2.99. Deverá permitir a criação de regras para acesso/bloqueio por subrede de origem e destino;

2.100. Atualizar a base de assinaturas de aplicações automaticamente;

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

2.102. A solução de controle de aplicação WEB deve criar regras granulares possibilitando adicionar tipos de aplicação WEB e categorias por regra, sendo assim criando controle granular de qualquer tipo de acesso não permitido pela empresa;

2.103. Deve implementar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e protocolos;

2.104. Caso a solução não tenha assinaturas pré-definida na solução a mesma deverá possibilitar a criação ou importação de assinaturas personalizadas para os seguintes tipos ou protocolos: HTTP, FTP, E-mail e extensão de arquivos;

2.105. O administrador deve ser capaz de configurar quais comandos FTP são aceitos e quais são bloqueados a partir de comandos FTP pré-definidos;

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

2.107. Deverá possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, uTorrent, etc.) possuindo granularidade de controle/políticas para os mesmos;

2.108. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Facebook e bloquear chat;

2.109. Deverá possibilitar a diferenciação de aplicações Proxies possuindo granularidade de controle/políticas para os mesmos;

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

- Nível de risco da aplicação.
- Categoria de aplicações.

FILTRO DE URL

2.111. Para prover maior visibilidade e controle dos acessos dos usuários do ambiente, deve ser incluído um módulo de filtro de URL integrado no firewall;

2.112. Possuir base contendo no mínimo 20 milhões de sites internet web já registrados e classificados com atualização automática;

2.113. Implementar filtro de conteúdo transparente para o protocolo HTTP, de forma a dispensar a configuração dos browsers das máquinas clientes.

2.114. A plataforma de proteção deve possuir as seguintes funcionalidades de filtro de URL:

2.115. Permitir a criação de listas personalizadas de URLs permitidas e bloqueadas (lista branca e lista negra) ;

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

2.117. Deve ser possível à criação de políticas por usuários, grupos de usuários, IP´s, redes e grupos de redes;

2.118. O mecanismo de Controle de aplicação Web/URL deve apresentar contagem de utilização de regra de acordo com a utilização (hit count);

2.119. Deverá permitir criar política de confirmação de acesso;

2.120. Deve possibilitar a inspeção de tráfego HTTPS (Inbound/Outbound), sendo que para a opção de Outbound não será necessário efetuar o "man-inthe- middle", ou seja, a solução deverá prover mecanismo que irá analisar a conexão HTTPS para verificar se a URL solicitada está na lista de permissões de acesso, de acordo com a política configurada;

2.121. O administrador poderá adicionar filtros por palavra-chave de modo específico;

2.122. Deverá permitir o bloqueio Web através de senha pré configurada pelo administrador

2.123. Deverá 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);

2.124. A solução deve fornecer um mecanismo para solicitação de categorização de URL caso esta não esteja categorizada ou categorizada incorretamente;

2.125. Suportar recurso de autenticação única para todo o ambiente de rede, ou seja, utilizando a plataforma de autenticação atual que pode ser de LDAP ou AD; o perfil de cada usuário deverá ser obtido automaticamente para o controle das políticas de Filtro de Conteúdo sem a necessidade de uma nova autenticação;

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

2.127. Suportar base ou cache de URLs local no appliance ou possibilitar a replicação da base de conhecimento de URLs do fabricante via instalação de máquina virtual, a infraestrutura da máquina virtual (VM) para uso desse recurso será fornecida pelo CONTRATANTE, evitando delay de comunicação/validação das URLs;

2.128. Possuir pelo menos 50 categorias de URLs;

2.129. Suporta a criação de categorias de URLs customizadas;

2.130. Suporta a exclusão de URLs do bloqueio, por categoria;

2.131. Deverá possibilitar a categorização ou recategorização de URL caso não esteja categorizada ou categorizada incorretamente;

2.132. A solução deverá permitir um mecanismo que permita sobrescrever as categorias de URL;

2.133. Permite a customização de página de bloqueio;

PROTEÇÃO CONTRA VIRUS E BOT-NETS

2.134. Deve possuir módulo de antivírus e anti-bot integrado no próprio appliance de segurança;

2.135. A solução de anti-virus integrada deve ter capacidade de analisar arquivos maiores que 1Gbps;

2.136. A solução deve possuir nuvem de inteligência proprietária do fabricante onde seja responsável em atualizar toda a base de segurança dos appliances através de assinaturas;

2.137. Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e qualquer outro mecanismo de redirecionamento de tráfego;

2.138. Implementar funcionalidade de detecção e bloqueio de callbacks;

2.139. A solução deverá ser capaz de detectar e bloquear comportamento suspeito ou anormal da rede;

2.140. A solução Antibot deve possuir mecanismo de detecção que inclui, reputação de endereço IP;

2.141. Implementar interface gráfica WEB segura, utilizando o protocolo HTTPS.

2.142. Implementar interface CLI segura através do protocolo SSH;

2.143. Possuir antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, IMAP, POP3, FTP, CIFS e TCP Stream;

2.144. A solução deve permitir criar regras de exceção de acordo com a proteção;

2.145. Deve possuir visualização na própria interface de gerenciamento referente aos top incidentes através de hosts ou incidentes referentes a incidentes de vírus e Bots;

2.146. Permitir o bloqueio de malwares (vírus, worms, spyware e etc);

2.147. A solução deve ser capaz de proteger contra ataques para DNS;

2.148. A solução deverá ser gerenciada a partir de uma console centralizada com políticas granulares

2.149. A solução deve ser capaz de prevenir acesso a websites maliciosos;

2.150. A solução deve ser capaz de realizar inspeção de tráfego SSL e SSH;

2.151. A solução deverá receber atualizações de um serviço baseado em cloud;

2.152. A solução deverá ser capaz de bloquear a entrada de arquivos maliciosos;

2.153. A solução Antivírus deverá suportar análise de arquivos que trafegam dentro do protocolo CIFS.

2.154. A solução deve suportar funcionalidade de GeoIP, ou seja, a capacidade de identificar, isolar e controlar tráfego baseado na localização (origem e/ou destino), incluindo a capacidade de configuração de listas customizadas para esta mesma finalidade;

PROTEÇÃO CONTRA ATAQUES AVANÇADOS

2.155. A solução deverá prover as funcionalidades de inspeção de tráfego de entrada e saída de malwares não conhecidos ou do tipo APT com filtro de ameaças avançadas e análise de execução em tempo real, e inspeção de tráfego de saída de callbacks;

2.156. Suportar os protocolos HTTP assim como inspeção de tráfego criptografado através de HTTPS e TLS;

2.157. A solução deve ser capaz de inspecionar o tráfego criptografado SSL e SSH;

2.158. Identificar e bloquear a existência de malware em comunicações de entrada e saída, incluindo destinos de servidores do tipo Comando e Controle;

2.159. Implementar mecanismo de bloqueio de vazamento não intencional de dados oriundos de máquinas existentes no ambiente LAN em tempo real;

2.160. Implementar detecção e bloqueio imediato de malwares que utilizem mecanismo de exploração em arquivos no formato PDF, sendo que a solução deve inspecionar arquivo PDF com até 10Mb;

2.161. Implementar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows e Android;

2.162. Conter ameaças de dia zero permitindo ao usuário final o recebimento dos arquivos livres de malware;

2.163. A tecnologia de máquina virtual deverá suportar diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso sem utilização de assinaturas;

2.164. A solução deve possuir nuvem de inteligência proprietária do fabricante onde seja responsável em atualizar toda a base de segurança dos appliance através de assinaturas;

2.165. Implementar a visualização dos resultados das análises de malwares de dia zero nos diferentes sistemas operacionais dos ambientes controlados (sandbox) suportados;

2.166. Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e qualquer outro mecanismo de redirecionamento de tráfego;

2.167. Conter ameaças avançadas de dia zero;

2.168. Toda análise deverá ser realizada de forma automatizada sem a necessidade de criação de regras específicas e/ou interação de um operador;

2.169. Implementar mecanismo do tipo múltiplas fases para verificação de malware e/ou códigos maliciosos;

2.170. Toda a análise e bloqueio de malwares e/ou códigos maliciosos deve ocorrer em tempo real. Não serão aceitas soluções que apenas detectam o malware e/ou códigos maliciosos;

2.171. Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx) e Android APKs no ambiente controlado;

2.172. Implementar a análise de arquivos executáveis, DLLs e ZIP em SSL no ambiente controlado;

2.173. Possuir antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, POP3, FTP, IMAP e CIFS;

2.174. Conter ameaças de dia zero de forma transparente para o usuário final;

2.175. Conter ameaças de dia zero através de tecnologias em nível de emulação e código de registro;

2.176. Implementar mecanismo de pesquisa por diferentes intervalos de tempo;

2.177. Conter ameaças de dia zero via tráfego de internet;

2.178. Permitir a contenção de ameaças de dia zero sem a alteração da infraestrutura de segurança;

2.179. Conter ameaças de dia zero que possam burlar o sistema operacional emulado;

2.180. A solução deve permitir a criação de White list baseado no MD5 do arquivo;

2.181. Conter ameaças de dia zero antes da execução e evasão de qualquer código malicioso;

2.182. Conter exploits avançados;

2.183. A análise “In Cloud” ou local deve prover informações sobre as ações do Malware na máquina infectada, informações sobre quais aplicações são utilizadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo Malware, gerar assinaturas de Antivírus e Antispyware automaticamente, definir URLs não confiáveis utilizadas pelo novo Malware e prover Informações sobre o usuário infectado (seu endereço IP e seu login de rede);

2.184. Suporte a submissão manual de arquivos para análise através do serviço de Sandbox;

ADMINISTRAÇÃO

2.185. Suportar políticas baseadas por grupos de usuários deverão ser suportadas pelo dispositivo.

2.186. Permitir a criação de perfis de administração distintos, de forma a possibilitar a definição de diversos administradores para o firewall, cada um responsável por determinadas tarefas da administração;

2.187. Fornecer gerência remota, com interface gráfica nativa;

2.188. A interface gráfica deverá possuir assistentes para facilitar a configuração inicial e a realização das tarefas mais comuns na administração do firewall, incluindo a configuração de VPN IPSECs, NAT, perfis de acesso e regras de filtragem;

2.189. Possuir mecanismo que permita a realização de cópias de segurança (backups) e sua posterior restauração remotamente, através da interface gráfica, sem necessidade de se reinicializar o sistema;

2.190. Possuir mecanismo para possibilitar a aplicação de correções e atualizações para o firewall remotamente através da interface gráfica;

2.191. Permitir a visualização em tempo real de todas as conexões TCP e sessões UDP que se encontrem ativas através do firewall e a remoção de qualquer uma destas sessões ou conexões;

2.192. Permitir a geração de gráficos em tempo real, representando os serviços mais utilizados e as máquinas mais acessadas em um dado momento;

2.193. Permitir a visualização de estatísticas do uso de CPU, memória da máquina onde o firewall está rodando e tráfego de rede em todas as interfaces do Firewall através da interface gráfica remota, em tempo real e em forma tabular e gráfica;

2.194. Permitir a conexão simultânea de vários administradores, sendo um deles com poderes de alteração de configurações e os demais apenas de visualização das mesmas. Permitir que o segundo ao se conectar possa enviar uma mensagem ao primeiro através da interface de administração.

2.195. Possibilitar o registro de toda a comunicação realizada através do firewall, e de todas as tentativas de abertura de sessões ou conexões que forem recusadas pelo mesmo;

2.196. Possuir interface orientada a linha de comando para a administração do firewall a partir do console ou conexão SSH sendo está múltiplas sessões simultâneas.

2.197. Possuir mecanismo que permita inspecionar o tráfego de rede em tempo real (sniffer) via interface gráfica, podendo opcionalmente exportar os dados visualizados para arquivo formato PCAP e permitindo a filtragem dos pacotes por protocolo, endereço IP origem e/ou destino e porta IP origem e/ou destino, usando uma linguagem textual;

2.198. Permitir a visualização do tráfego de rede em tempo real tanto nas interfaces de rede do Firewall quando nos pontos internos do mesmo: anterior e posterior à filtragem de pacotes, onde o efeito do NAT (tradução de endereços) é eliminado;

2.199. Possuir sistema de respostas automáticas que possibilite alertar imediatamente o administrador através de e-mails, janelas de alerta na interface gráfica, execução de programas e envio de Traps SNMP;

RELATÓRIOS

2.200. Ser capaz de visualizar, de forma direta no appliance e em tempo real, as aplicações mais utilizadas, os usuários que mais estão utilizando estes recursos informando sua sessão, total de pacotes enviados, total de bytes enviados e média de utilização em Kbps, URLs acessadas e ameaças identificadas.

2.201. Possibilitar a geração de pelo menos os seguintes tipos de relatório com cruzamento de informações, mostrados em formato HTML: máquinas acessadas X serviços bloqueados, usuários X URLs acessadas, usuários X categorias Web bloqueadas (em caso de utilização de um filtro de conteúdo Web);

2.202. Possibilitar a geração de pelo menos os seguintes tipos de relatório, mostrados em formato HTML: máquinas mais acessadas, serviços mais utilizados, usuários que mais utilizaram serviços, URLs mais visualizadas, ou categorias Web mais acessadas (em caso de existência de um filtro de conteúdo Web), maiores emissores e receptores de e-mail;

2.203. Permitir o envio dos relatórios, através de e-mail para usuários pré-definidos;

2.204. Possuir relatórios pré-definidos na solução e permitir a criação de relatórios customizados;

2.205. Possibilitar a geração dos relatórios sob demanda e através de agendamento diário, semanal e mensal. No caso de agendamento, os relatórios deverão ser publicados de forma automática

2.206. Disponibilizar download dos relatórios gerados;

3. Garantia, Suporte e Licenciamento

3.1. Deve contemplar suporte do Fabricante pelo período vigente ao contrato.

3.2. O suporte do fabricante deve ter um sistema de abertura de chamados para acompanhamento – funcionando 24 horas por dia e 7 dias por semana. Para atendimento telefônico, deve operar em língua Portuguesa pelo menos em regime 8x5.

3.3. Deve assegurar a utilização de novas versões de software da solução sem ônus a CONTRATANTE, sempre que esta estiver disponível oficialmente.

4. Conformidade

4.1. O Fabricante deve comprovar participação no MAPP da Microsoft;

4.2. A tecnologia deve possuir pelo menos uma certificação da ICSA Labs, ICSA Firewall ou Antivírus;

4.3. O fabricante da solução deverá ser avaliado pela NSS Labs (Network Security Services) no desempenho do Next Generation Firewall Comparative Analysis mais recente, estando no “Security Value Map” acima de 90 % (noventa por cento) da avaliação de segurança efetiva.

4.4. O fornecimento dos produtos e seus licenciamentos devem ser entregues através de empresa credenciada e autorizada pelo fabricante. Isto deve ser comprovada através de carta de reconhecimento assinada pelo representante legal do fabricante no Brasil

4.5. Deve ser homologado pela ANATEL.

5. DO ENCAMINHAMENTO E ACEITABILIDADE DA PROPOSTA

5.1. A proposta final deverá conter as seguintes informações:

5.1.1. 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.

5.1.2. 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;

5.1.3. Ter validade não inferior a 60 (sessenta) dias, contados a partir da data de sua apresentação;

5.1.4. DECLARAÇÃO de que os produtos fornecidos são novos, de primeiro uso e estão em linha de fabricação na data de abertura das propostas;

5.1.5. DECLARAÇÃO de que a empresa fornecedora é parceira oficial e tem condições comercializar, instalar, configurar e prestar manutenção na solução ofertada.

5.1.6. 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.

5.1.7. 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.

5.1.8. Declaração, certificado ou contrato de distribuição emitido pelo fabricante dos produtos, comprovando que a empresa proponente faz parte do seu programa de parceria.

5.1.9. 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.

5.1.10. 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.

5.1.11. Todas as especificações do objeto contidas na proposta vinculam a Contratada.

5.1.12. 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.

TABELA DE ENDEREÇOS – ANEXO II

LINHAS ANALOGICAS: TABELA 1

SERVIÇO	Classe de Serviço	Núm. Linha	Endereço	CEP	Município	UF
TERMINAL	LINA	1434782135	R BARROSO,ALM, 75	17690000	BASTOS	SP
TERMINAL	LINA	1434782148	R PEDRO I,DOM, 19	17690000	BASTOS	SP
TERMINAL	LINA	1434782609	R CAXIAS,DQ, 600	17690000	BASTOS	SP
TERMINAL	LINA	1434781955	R RUI BARBOSA, 1217	17690000	BASTOS	SP
TERMINAL	LINA	1434781821	AV GASPAR RICARDO, 1800	17690000	BASTOS	SP
TERMINAL	LINA	1434782096	R UNIAO, SN	17690000	BASTOS	SP
TERMINAL	LINA	1434786814	AV DEZOITO DE JUNHO, 175	17690000	BASTOS	SP
TERMINAL	LINA	1434783103	R AMAZONAS, 65	17690000	BASTOS	SP
TERMINAL	LINA	1434784005	R VARGAS,PRES, 488	17690000	BASTOS	SP
TERMINAL	LINA	1434782740	R EMILIO MONTEIRO, 246	17690000	BASTOS	SP
TERMINAL	LINA	1434783554	R FLORIANO PEIXOTO,MAL, 545	17690000	BASTOS	SP
TERMINAL	LINA	1434783237	R SATOSHI NAGAHASHI, 800	17690000	BASTOS	SP
TERMINAL	LINA	1434782281	R OSORIO,GAL, 1006	17690000	BASTOS	SP
TERMINAL	LINA	1434782507	R FLORIANO PEIXOTO,MAL, 790	17690000	BASTOS	SP
TERMINAL	LINA	1434781059	AV DEZOITO DE JUNHO, 461	17690000	BASTOS	SP
TERMINAL	LINA	1434781115	R CAXIAS,DQ, 600	17690000	BASTOS	SP
TERMINAL	LINA	1434781600	AV DEZOITO DE JUNHO, 335	17690000	BASTOS	SP
TERMINAL	LINA	1434784515	R ADHEMAR DE BARROS, 800	17690000	BASTOS	SP
TERMINAL	LINA	1434781608	R OSVALDO CRUZ, 878	17690000	BASTOS	SP
TERMINAL	LINA	1434781611	R SENJIRO HATANAKA, 99	17690000	BASTOS	SP
TERMINAL	LINA	1434781621	AV GASPAR RICARDO, 15000	17690000	BASTOS	SP
TERMINAL	LINA	1434782155	R CAMPOS SALLES, 355	17690000	BASTOS	SP
TERMINAL	LINA	1434781650	AV GASPAR RICARDO, 1700	17690000	BASTOS	SP
TERMINAL	LINA	1434781604	R ADHEMAR DE BARROS, 530	17690000	BASTOS	SP
TERMINAL	LINA	1434782066	AV DEZOITO DE JUNHO, 90	17690000	BASTOS	SP
TERMINAL	LINA	1434781200	R TUCANOS, 315	17690000	BASTOS	SP
TERMINAL	LINA	1434781790	AV DEZOITO DE JUNHO, 251	17690000	BASTOS	SP
TERMINAL	LINA	1434782200	AV GASPAR RICARDO, 1800	17690000	BASTOS	SP
TERMINAL	LINA	1434786690	R JOSE CANDIDO MANCILHIA, 125	17690000	BASTOS	SP
TERMINAL	LINA	1434781613	AV GASPAR RICARDO, 1800	17690000	BASTOS	SP
TERMINAL	LINA	1434785066	R SETE DE SETEMBRO, 455	17690000	BASTOS	SP
TERMINAL	LINA	1434783156	AV DEZOITO DE JUNHO, 162	17690000	BASTOS	SP
TERMINAL	LINA	1434782376	R VARGAS,PRES, 1040	17690000	BASTOS	SP
TERMINAL	LINA	1434781331	R AMAZONAS, 65	17690000	BASTOS	SP
TERMINAL	LINA	1434785004	R BRASILIA, 320	17690000	BASTOS	SP
TERMINAL	LINA	1434784007	R BEM TE VI, 165	17690000	BASTOS	SP
TERMINAL	LINA	1434786557	AV GASPAR RICARDO, 757	17690000	BASTOS	SP
TERMINAL	LINA	1434787013	R CIDADE DE KUMANO, 380	17690000	BASTOS	SP
TERMINAL	LINA	1434786941	R OSVALDO CRUZ, 878	17690000	BASTOS	SP
TERMINAL	LINA	1434781438	R BARROSO,ALM, 75	17690000	BASTOS	SP
TERMINAL	LINA	1434786186	R OSORIO,GAL, 894	17690000	BASTOS	SP
TERMINAL	LINA	1434781868	R EMILIO MONTEIRO, 515	17690000	BASTOS	SP
TERMINAL	LINA	1434786169	R SETE DE SETEMBRO, 445	17690000	BASTOS	SP
TERMINAL	LINA	1434782470	R CAXIAS,DQ, 640	17690000	BASTOS	SP
TERMINAL	LINA	1434783307	AV DEZOITO DE JUNHO, 162	17690000	BASTOS	SP
TERMINAL	LINA	1434781322	R VARGAS,PRES, 400	17690000	BASTOS	SP
TERMINAL	LINA	1434781648	R PERNAMBUCO, 100	17690000	BASTOS	SP
TERMINAL	LINA	1434786401	R SETE DE SETEMBRO, 339	17690000	BASTOS	SP
TERMINAL	LINA	1434786449	R BEM TE VI, 25	17690000	BASTOS	SP
TERMINAL	LINA	1434781969	R SETE DE SETEMBRO, 455	17690000	BASTOS	SP

PARECER
Examinado e aprovado pela Secretaria Mun.dos
Negócios Juridicos de acordo com a Lei 8.666/93
Atualizada pela Lei 8.883/94
Bastos-SP, 23 de outubro de 2019
Rafael Teixeira Sebastiani – OAB/SP 355751
Procurador Jurídico

TRONCOS DIGITAIS : TABELA 2

Produto	Canais	Ramais	Núm. Linha	Endereço	CEP	Município	UF
DDR	15	15	1434789800	R ADHEMAR DE BARROS, 530	17690000	BASTOS	SP
DDR	10	10	1434781115	R CAXIAS,DQ, 600	17690000	BASTOS	SP
DDR	10	10	1434786169	R SETE DE SETEMBRO, 445	17690000	BASTOS	SP

ACESSO LINK DEDICADO: TABELA 3

Produto	Velocidade	Qtd. de Acesso Dados	Endereço	CEP	Município	UF
IP DEDICADO	100 MBPS	1	RUA ADHEMAR DE BARROS, 600	17690000	BASTOS	SP

TABELA DESCRITIVA – ANEXO III

MENSALIDADE DOS SERVIÇOS				
	QTDE	**Valor Unitário (R$)**	**Valor Mensal (R$)**	**Valor 12 Meses (R$)**
Linhas Convencionais	50	R$ -	R$ -	R$ -
Troncos Digitais 10 canais	2	R$ -	R$ -	R$ -
Ramais DDR	10	R$ -	R$ -	R$ -
Troncos Digitais 15 canais	1	R$ -	R$ -	R$ -
Ramais DDR	15	R$ -	R$ -	R$ -
Pacote de minutos Ilimitado Nacional	1	R$ -	R$ -	R$ -
Pacote de minutos Ilimitado Nacional	2	R$ -	R$ -	R$ -
Internet Dedicada 100MB	1	R$ -	R$ -	R$ -
Serviço de Segurança	1	R$ -	R$ -	R$ -
		sub total 1	**R$ -**	**R$ -**
LOCAL				
TIPO Terminal	**QTDE**	**Valor Unitário (R$)**	**Valor Mensal (R$)**	**Valor 12 Meses (R$)**
Minuto fixo - fixo (local) TERMINAL	7.000	R$ -	R$ -	R$ -
Minuto Local (VC1) TERMINAL	1000	R$ -	R$ -	R$ -
TIPO DDR	**QTDE**	**Valor Unitário (R$)**	**Valor Mensal (R$)**	**Valor 12 Meses (R$)**
Minuto fixo - fixo (local) DDR	10.000	R$ -	R$ -	R$ -
Minuto Local (VC1) DDR	3000	R$ -	R$ -	R$ -
		sub total 2	**R$ -**	**R$ -**
LONGA DISTÂNCIA				
TIPO Terminal	**QTDE**	**Valor Unitário (R$)**	**Valor Mensal (R$)**	**Valor 12 Meses (R$)**
Minuto fixo - fixo Intra-regional	1.000	R$ -	R$ -	R$ -
Minuto fixo - móvel Intra-regional (VC2)	100	R$ -	R$ -	R$ -
Minuto fixo - fixo Inter-regional	100	R$ -	R$ -	R$ -
Minuto fixo - móvel Inter-regional (VC3)	10	R$ -	R$ -	R$ -
TIPO DDR	**QTDE**	**Valor Unitário (R$)**	**Valor Mensal (R$)**	**Valor 12 Meses (R$)**
Minuto fixo - fixo Intra-regional	2.500	R$ -	R$ -	R$ -
Minuto fixo - móvel Intra-regional (VC2)	280	R$ -	R$ -	R$ -
Minuto fixo - fixo Inter-regional	120	R$ -	R$ -	R$ -
Minuto fixo - móvel Inter-regional (VC3)	35	R$ -	R$ -	R$ -
		sub total 3	**R$ -**	**R$ -**
Total mensal (1+2+3)			**R$**	**-**

PARECER
Examinado e aprovado pela Secretaria Mun.dos
Negócios Juridicos de acordo com a Lei 8.666/93
Atualizada pela Lei 8.883/94
Bastos-SP, 23 de outubro de 2019
Rafael Teixeira Sebastiani – OAB/SP 355751
Procurador Jurídico

PREFEITURA DO MUNICÍPIO DE BASTOS
RUA ADHEMAR DE BARROS, 530
CNPJ 45 547 403/0001-93 **CONTRATO Nº**
PROCESSO Nº

MINUTA PARA CONTRATAÇÃO DE EMPRESA ESPECIALIZADA PARA PRESTAÇÃO DE SERVIÇOS DE TELECOMUNICAÇÕES E TECNOLOGIA DA INFORMAÇÃO, SENDO ELES: (1) PRESTAÇÃO DE SERVIÇO DE TELECOMUNICAÇÕES STFC (SERVIÇO TELEFÔNICO FIXO COMUTADO) NAS MODALIDADES ANALÓGICO E DIGITAL, (2) FORNECIMENTO DE LINK DEDICADO DE ACESSO À INTERNET, (3) FORNECIMENTO E IMPLANTAÇÃO DE SOLUÇÃO DE SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO, NOS TERMOS DAS CONCESSÕES OUTORGADAS PELA AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES – ANATEL DESTINADOS AO USO DA PREFEITURA, QUE ENTRE SI CELEBRAM A PREFEITURA DO MUNICÍPIO DE BASTOS E A FIRMA ...

Pela presente Minuta de Contrato, objeto do Pregão Presencial nº098/2019, para CONTRATAÇÃO DE EMPRESA ESPECIALIZADA PARA PRESTAÇÃO DE SERVIÇOS DE TELECOMUNICAÇÕES E TECNOLOGIA DA INFORMAÇÃO, SENDO ELES: (1) PRESTAÇÃO DE SERVIÇO DE TELECOMUNICAÇÕES STFC (SERVIÇO TELEFÔNICO FIXO COMUTADO) NAS MODALIDADES ANALÓGICO E DIGITAL, (2) FORNECIMENTO DE LINK DEDICADO DE ACESSO À INTERNET, (3) FORNECIMENTO E IMPLANTAÇÃO DE SOLUÇÃO DE SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO, NOS TERMOS DAS CONCESSÕES OUTORGADAS PELA AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES – ANATEL, destinados ao uso da Prefeitura, pelo regime de execução por preço global, sendo o tipo de licitação a de menor preço, regido em todos os seus termos pelas Leis

PARECER
Examinado e aprovado pela Secretaria Mun.dos
Negócios Juridicos de acordo com a Lei 8.666/93
Atualizada pela Lei 8.883/94
Bastos-SP, 23 de outubro de 2019
Rafael Teixeira Sebastiani – OAB/SP 355751
Procurador Jurídico

Federais n.ºs 10.520 de 17 de julho de 2002, 8.666/93 de 23 de junho de 1993 alterada pela Lei Federal n.º 8.883/94 e introduções posteriores, Decreto nº7.892 de 23 de janeiro de 2013, Lei Municipal n.º 1.980/07 de 16 de outubro de 2007, Decreto Municipal nº597/09 de 26 de janeiro de 2009 e demais normas regulamentares aplicáveis à espécie que entre si celebram de um lado a PREFEITURA DO MUNICÍPIO DE BASTOS, doravante denominada simplesmente **CONTRATANTE**, representada pelo seu Prefeito Municipal **Sr. MANOEL IRONIDES ROSA**, e de outro lado a Empresa ...**,** Inscrita no CNPJ sob o nº ... e Inscrição Estadual nº ..., com sede na Rua ..., na Cidade de ..., Estado de ..., doravante denominada simplesmente **CONTRATADA**, representada pelo(s) sócio(s) proprietário(s) Sr(s) ... residente e domiciliado na Cidade de..., Estado de..., têm entre si justos e acertados as Cláusulas abaixo, que reciprocamente se comprometem a cumprir e a respeitar:-

CLÁUSULA PRIMEIRA

Constitui objeto do presente Contrato, a CONTRATAÇÃO DE EMPRESA ESPECIALIZADA PARA PRESTAÇÃO DE SERVIÇOS DE TELECOMUNICAÇÕES E TECNOLOGIA DA INFORMAÇÃO, SENDO ELES: (1) PRESTAÇÃO DE SERVIÇO DE TELECOMUNICAÇÕES STFC (SERVIÇO TELEFÔNICO FIXO COMUTADO) NAS MODALIDADES ANALÓGICO E DIGITAL, (2) FORNECIMENTO DE LINK DEDICADO DE ACESSO À INTERNET, (3) FORNECIMENTO E IMPLANTAÇÃO DE SOLUÇÃO DE SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO, NOS TERMOS DAS CONCESSÕES OUTORGADAS PELA AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES – ANATEL, a seguir discriminados:-

OBJETO:

CONTRATAÇÃO DE EMPRESA ESPECIALIZADA PARA PRESTAÇÃO DE SERVIÇOS DE TELECOMUNICAÇÕES E TECNOLOGIA DA INFORMAÇÃO, SENDO ELES: (1) PRESTAÇÃO DE SERVIÇO DE TELECOMUNICAÇÕES STFC (SERVIÇO TELEFÔNICO FIXO COMUTADO) NAS MODALIDADES ANALÓGICO E DIGITAL, (2) FORNECIMENTO DE LINK DEDICADO DE ACESSO À INTERNET, (3) FORNECIMENTO E IMPLANTAÇÃO DE SOLUÇÃO DE SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO, NOS TERMOS DAS CONCESSÕES OUTORGADAS PELA AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES – ANATEL.

ESPECIFICAÇÕES TECNICAS:

1. Dos Acessos

1.1. Linhas telefonicas

1.1.1. Fornecer linhas telefônicas analógicas nas quantidades e endereços estabelecidos na **Tabela 1.**

1.1.2. Ativar novas linhas telefônicas conforme necessidade da CONTRATANTE;

1.1.3. Desativar linhas telefônicas que estiverem em operação conforme necessidade da CONTRATANTE;

1.1.4. Possibilidade de serviços adicionais como identificador de chamadas, busca entre terminais, bloqueio de ligações a cobrar ou DDD, DDI e celular conforme necessidade da CONTRATANTE.

1.1.5. Novas linhas telefônicas deverão ser instaladas no prazo máximo de 10 dias;

1.1.6. Devem ser telealimentadas, afim de garantir a comunicação mesmo na falta de energia elétrica.

1.1.7. Tecnologias alternativas como FWT (Fixed wireless Terminal) serão permitidas somente para endereços onde não houver disponibilidade de par metálico.

1.1.8. Central de Atendimento 24h por dias, 365 dias por ano através de um número 0800;

1.1.9. A CONTRATADA deverá manter a mesma numeração atualmente utilizada (números de telefone) conforme critérios da Portabilidade regulamentada pela ANATEL, para os números relacionados no Anexo I, além de outros que tiverem sua inclusão neste certame.

1.1.10. Nos casos onde não for possível a instalação por par metálico ou FWT, que dependam de projeto de infraestrutura, deverá ser apresentado para a CONTRATANTE que será responsável pelo custo do projeto.

1.2. Tronco Digital E1

1.2.1. Fornecer tronco digital E1 e faixas DDR nas quantidades estabelecidas no **Anexo II – Tabela 2;**

1.2.2. Interface tipo G.703

1.2.3. Sinalização de Linha tipo R2D

1.2.4. Sinalização de Registro tipo MFC 5C ou 5S

1.2.5. Ativar e desativar troncos conforme necessidade da CONTRATANTE e segundo o limite estabelecido na lei 8.666;

1.2.6. Prazo de instalação de 90 dias;

1.2.7. Disponibilidade mensal (SLA - Service level agreement) de 99% ao mês;

1.2.8. Início de atendimento em caso de defeito em até 4 horas

1.2.9. Meio de atendimento em par-metálico, fibra-óptica;

1.2.10. Em casos onde for constatada inviabilidade de instalação a CONTRATADA deverá encaminhar as condições de atendimento (custo, prazo e meio) para análise da CONTRATANTE e será objeto de aditivo contratual.

1.2.11. Central de Atendimento 24h por dias, 365 dias por ano através de um numero 0800;

1.2.12. Mudança de endereço de acessos instalados tem o mesmo prazo de instalação de novos acessos;

1.2.13. A CONTRATADA deverá manter a mesma numeração atualmente utilizada (números de telefone) conforme critérios da Portabilidade regulamentada pela ANATEL, para os números relacionados no **Anexo II – Tabela 2**, além de outros que tiverem sua inclusão neste certame.

2. Do tráfego Telefônico

2.1. Método

2.1.1. Conforme especificações mínimas estabelecidas pelo órgão regulador;

2.1.2. Informar os custos de assinatura individuais das linhas telefonicas, troncos digitais , faixas DDR e serviço 0800;

2.1.3. A tarifação das chamadas deverá ser realizada em minutos;

2.1.4. As tarifas utilizadas deverão ter como base aqueles constantes do Plano básico de serviços ou do Plano alternativo de serviços, regulamentado para o setor de telecomunicação e informado através do preenchimento da Proposta Comercial**,** com todos os impostos regulamentados e descontos concedidos a critério da Licitante;

2.1.5. As mensalidades para as linhas analógicas deverão contemplar os custos de 150 (cento e cinquenta) minutos para ligação local fixo-fixo (inclusos nesta cotação);

2.2. Perfil de tráfego

2.2.1. Deverão ser considerados os volumes de chamadas indicadas no **Anexo** como referência orientativa para apresentação de proposta;

2.2.2. O Perfil de Tráfego e seus custos **(Anexo III)**, compõe-se de uma ESTIMATIVA, em minutos e em valores, baseadas nas faturas das contas telefônicas da CONTRATANTE relativa às chamadas originadas em seu âmbito, bem como outros serviços atualmente utilizados;

2.2.3. O Perfil de Tráfego do **Anexo III**, servirá tão somente de subsídio para análise da proposta global mais vantajosa e portanto, não implicam em qualquer compromisso futuro ou restrição quantitativa de uso para a CONTRATANTE.

2.3. Da fatura

2.3.1. As faturas de cada serviço devem ser encaminhadas via papel, individualizada por linha seja analógica ou digital, com valor total e o respectivo descritivo com os valores das ligações;

2.4. Responsabilidades da contratante

Toda a infra-estrutura civil, elétrica, ar condicionado, leitos de passagem de cabos, rede interna (cabeamento horizontal) e serviços são de responsabilidade da contratante, incluindo a adequação conforme as necessidades de implantação do projeto, bem como disponibilizar o PABX com interface para E1 30 canais

Da mesma forma, será de responsabilidade do CONTRATANTE reparar ou refazer os acabamentos necessários para instalação do objeto pela CONTRATADA.

2.4.1. Requisitos mínimos sugeridos

2.4.1.1. Circuito Bifásico 220 / 110V (suportado por no-break, com disjuntor de proteção 50 A) .

2.4.1.2. Rede estabilizada, ininterrupta, suportada por gerador, para garantir perfeito funcionamento dos equipamentos;

2.4.1.3. Infra-estrutura para que o acessos digitais (E1) ou analógicos (linhas telefônicas) cheguem até os equipamentos PABX fornecidos;

2.4.1.4. Quadro de Força com circuitos independentes e exclusivos para os equipamentos com disjuntores de 110 e 220V;

2.4.1.5. Cabeamento vertical e horizontal para a ativação dos ramais;

2.4.1.6. Jumpeamento do Bloco PABX para rede cliente;

2.4.1.7. Disponibilizar local preparado para acomodar o PABX e seus periféricos;

2.4.1.8. Aterramento < 10 ohms bitola 16 mm, conforme norma NBR 5410 de 1997da ABNT em ponto único para equalização de potencial, conforme norma vigente - NBR5410/NB - 3 - 1997;

2.4.1.9. Piso e paredes com acabamento final e vedação contra pó e umidade;

2.4.1.10. Extintor de incêndio obedecendo às normas do corpo de bombeiros;

2.4.1.11. Ambiente com climatização adequada, boa iluminação e acesso restrito;

2.4.2. Prazo e condições de instalação

2.4.2.1. O escopo de instalação está restrito a ativação e teste dos equipamentos fornecidos, toda a infra-estrutura necessária e quaisquer programações diferenciadas para interligação de sistemas, são de responsabilidade do CONTRATANTE;

2.4.2.2. O prazo de instalação é de 30 (trinta) dias após assinatura do contrato, prorrogáveis por mais 30 (trinta) dias, à critério da Administração;

2.4.3. Condições de manutenção

Os serviços especializados na rede interna: manutenção, configuração e ampliação são de responsabilidade do CONTRATANTE;

3.3– LOCAL, PRAZO E CONDIÇÕES DE ENTREGA:

3.3.1 - A habilitação das linhas e o consequente início da prestação dos serviços contratados deverão ocorrer no prazo máximo de 30 (trinta) dias corridos, podendo ser prorrogados por mais 15 dias mediante justificativa, contados a partir da data de entrega dos Chips e caso a Prefeitura solicite a portabilidade das linhas o prazo será o mínimo previsto pela ANATEL.

3.4- DO PRAZO DE VIGÊNCIA DO CONTRATO

3.4.1– O contrato terá vigência por doze (12) meses, iniciando-se a partir de sua assinatura, podendo ser prorrogado a critério da Prefeitura Municipal de Borborema com fulcro no artigo 57, inciso II, da Lei nº 8.666/93 e legislações posteriores.

Link dedicado de Dados (internet)

Link dedicado de dados (Internet) com velocidade informada no Anexo III, com as seguintes especificações mínimas:

– Acesso:

– O link deverá ser fornecido obrigatoriamente através de fibra óptica;

– Deverá ser bidirecional e simétrico na velocidade mínima de 30 Mbps;

– O uso de Fibra Óptica como meio físico de transporte dos dados deverá ser utilizado em todos os enlaces (trajeto) desde o backbone da operadora de telecomunicações, até o roteador instalado dentro do datacenter da CONTRATANTE;

– Velocidade mínima de 96,8% da velocidade nominal, tanto para download como para upload;

– Disponibilidade real mínima de 99,2% (SLA);

– A CONTRATANTE não terá qualquer tipo de limitação quanto a quantidade (em bytes) e conteúdo da informação trafegada no acesso;

– Possuir taxa de perda de pacotes menor ou igual a 1%;

– Latência média de no máximo 220 ms;

– Fornecimento mínimo de 6 endereços IP (V4) para cada link;

– A CONTRATADA deverá possuir Termo de Autorização para a prestação de Serviço Comunicação Multimídia (SCM) outorgado pela ANATEL;

– A CONTRATADA deverá possuir central de atendimento 24 horas por dia, 365 dias por ano, através de um número 0800;

– Em caso de defeito, o início do atendimento deverá ser de no máximo 4 horas;

– O Acesso deve ser realizado sem necessidade de provedor;

– Painel web ou software disponibilizado pela CONTRATADA, para acompanhamento, gerenciamento dos links de dados, tais como, criação de relatórios de métricas de uso de dados, métricas de tempo de reparo, etc.

– Saída para backbone internacional própria;
– Saída internacional agregada maior ou igual a 5 Gbps;
– Latência média menor ou igual à 75 ms;
– Perda de pacotes menor ou igual a 1%;
– Disponibilidade mensal do backbone internacional maior ou igual à 99,7%;

– Dos equipamentos (roteadores).
– O roteador será fornecido pela CONTRATADA, com instalação, configuração e gerencia;
– A configuração será executada para que a rede de computadores da contratante possua acesso a internet;
– Possuir quantidade mínima de memória que atenda a velocidade funcionalidades deste item, em conformidade com as recomendações do fabricante;
– Possuir protocolo de gerenciamento SNMP;
– Todos os roteadores deverão ter capacidade para suportar tráfego com banda completamente ocupada, sem exceder a 80% de utilização de CPU e memória;
– Responder por todas as normas definidas pela Agencia Nacional de Telecomunicações – ANATEL;

2. – Prazo e condições de instalação.
2.1 – O escopo de instalação esta restrito a ativação e teste dos equipamentos fornecidos, toda a infraestrutura necessária e quaisquer programações diferenciadas para interligação de sistemas, são de responsabilidade da CONTRATANTE;
2.2 – O prazo máximo de instalação é de 90 (noventa) dias após assinatura do contrato, podendo ser prorrogado por mais 30 dias;

SERVIÇO GERENCIADO DE SEGURANÇA

Contratação de empresa especializada para fornecimento de MSS (*Managed Security Services*) sobre a solução de segurança com as funcionalidades descritas em **ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO**, contemplando serviços de instalação, configuração, manutenção, suporte técnico remoto, monitoramento e gerenciamento na modalidade 24x7x365, pelo período de 36 meses.

2 DESCRIÇÃO DO SERVIÇO

3.2. Solução de Gerenciamento com fornecimento de hardware e software

3.2.1. A **CONTRATADA** deverá fornecer, em regime de comodato, conforme descrito em **ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO**, necessária para a realização dos

serviços, em regime 24x7x365 para a solução ofertada durante a vigência do contrato.

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

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

3.3. Gerenciamento/Manutenção

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

3.4. Serviço de comunicação de dados

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

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

3.5. Infraestrutura mínima necessária.

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

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

3.5.3. Responsabilidades do SOC

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

3.5.3.1.1. Segurança física: mecanismos de monitoração e registro de todo e qualquer acesso ao SOC, utilizando-se de câmeras de segurança;

3.5.3.1.2. Acesso ao SOC controlado por mecanismos de autenticação forte (pelo menos autenticação de dois fatores); ambiente isolado de outros que não sejam destinados à operacionalização e controle de segurança;

3.5.3.1.3. Mecanismos de prevenção, detecção e combate a incêndios;

3.5.3.1.4. Política de acesso lógico: possuir autenticação forte no acesso aos equipamentos que estarão nas dependências da **CONTRATANTE**, com usuários segregados por função e registros para controle de auditoria;

3.5.3.1.5. Possuir políticas definidas para criação, exclusão e manutenção de chaves, senhas e perfis de acesso.

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

3.5.4.1. <u>MANUTENÇÃO</u>

3.5.4.1.1. Fornecer apoio técnico necessário para realizar o diagnóstico de eventos de falha em seus ativos de segurança. Através da análise dos logs do equipamento, o SOC deverá determinar se houve alguma avaria em um dos componentes de hardware da solução e identificar a necessidade ou não de sua substituição.

3.5.4.1.2. Efetuar o processo de RMA (sigla em inglês de *return merchandise authorization*).

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

3.5.4.2. <u>SUPERVISÃO</u>

3.5.4.2.1. Efetuar a monitoração constante da capacidade e da disponibilidade da infraestrutura de segurança contratada.

3.5.4.2.2. Compreender as atuais demandas sobre os recursos de segurança e criar previsões para futuras solicitações quando necessário.

3.5.4.2.3. Avaliar se o nível de disponibilidade é sustentável, permitindo o negócio atingir seus objetivos de forma consistente.

3.5.4.2.4. Ter uma arquitetura de monitoração, baseada em solução que utiliza o protocolo SNMP para realizar os *healthchecks*.

3.5.4.2.5. Processar e disponibilizar em relatórios mensais os dados coletados.

3.5.4.2.6. Identificar que o componente atingiu certo nível de utilização (threshold).

3.5.4.2.7. Alertar e encaminhar para os técnicos responsáveis pela administração.

3.5.4.2.8. Acompanhar a saúde dos dispositivos supervisionando-os 24x7.

3.5.4.2.9. Comunicar ao **CONTRATANTE**, anomalias quando um componente monitorado apresentar índices não usuais.

3.5.4.2.10. Prover a monitorização da saúde dos dispositivos

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

3.5.4.3. ADMINISTRAÇÃO

3.5.4.3.1. Realizar a operação remota, gestão de mudança e gestão de configuração dos dispositivos de segurança contratado.

3.5.4.3.2. Resolução nos incidentes de segurança que ocorrem nos elementos administrado (s), detectados pelo monitoramento ou que sejam informados pela **CONTRATANTE**.

3.5.4.3.3. Planejar e realizar implementação de mudanças no ambiente contratado e gerenciado, sejam elas solicitadas pelo **CONTRATANTE** ou mesmo por recomendação da própria **CONTRATADA**, baseados nas melhores práticas de gestão.

3.5.4.3.4. Efetuar tarefas operacionais básicas, tais como executar *backup/restore* de configurações e gerenciamento do ambiente contratado.

3.5.4.3.5. Garantir o correto funcionamento dos dispositivos administrados.

3.5.4.3.6. Manter e atualizar o ambiente contratado com o software do dispositivo na versão mais atual recomendada pelo fabricante.

3.5.4.3.7. Efetuar aplicação de patches para a resolução de incidentes, correção de vulnerabilidades e prevenção de incidentes de segurança.

3.5.4.3.8. Efetuar atualização de software e patches somente se e quando autorizada pela **CONTRATANTE**, através do processo de gestão da mudança.

3.5.4.3.9. Informar ao **CONTRATANTE** dos possíveis riscos de segurança identificados através da administração da infraestrutura ou através das ferramentas de administração.

3.5.4.3.10. Atender as dúvidas e solicitações de segurança da **CONTRATANTE**.

3.5.4.3.11. Acompanhar e encaminhar os chamados através de ferramenta.

3.6. Implantação da Solução:

3.6.1. A implantação da solução de hardware e software deverá ser realizada no prazo de até 120 (cento e vinte dias) dias da contratação, mediante entrega de cronograma, detalhando as fases do projeto de implantação. Esse cronograma deverá ser aprovado pelo **CONTRATANTE**, sendo a implantação iniciada somente após esta aprovação.

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

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

3.6.2.2. Implantação: Relatório de implantação;

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

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

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

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

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

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

4. PRESTAÇÃO DOS SERVIÇOS

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

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

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

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

4.2.1.2. Definir as estratégias, políticas e regras a serem implantadas, e analisar/aprovar as solicitações;

4.2.1.3. Tomar as providências necessárias, em caso da ocorrência de algum incidente (análise dos logs, rastreamento da ocorrência).

4.2.2. A **CONTRATANTE** poderá realizar inspeção nas instalações do SOC, com o objetivo de verificar a segurança física e lógica do ambiente, a qualquer tempo com a **CONTRATADA**.

4.3. Ocorrência de Incidentes

4.3.1. No caso de detecção de algum incidente de segurança, a **CONTRATADA** deverá notificar a **CONTRATANTE** dentro do período estabelecido no SLA, para que sejam tomadas as medidas corretivas e legais necessárias.

4.3.1.1. São considerados incidentes de segurança: os acessos indevidos, instalação de códigos maliciosos, ataques por força bruta, ou qualquer outra ação que vise prejudicar a funcionalidade ou a disponibilidade dos serviços da **CONTRATANTE**.

4.3.2. A **CONTRATADA** comunicará imediatamente a **CONTRATANTE**, para que possam ser tomadas ações preventivas, nos casos de tentativas, sem sucesso, de acessos indevidos, de instalação de códigos maliciosos, ou de qualquer outra ação que venha pôr em risco a segurança do ambiente do **CONTRATANTE**, em que seja evidenciada a insistência, por parte da pessoa mal-intencionada.

4.3.3. A **CONTRATADA** disponibilizará todas as informações necessárias (origem do ataque, tipo de ataque, data e hora, logs, etc.) para que sejam apurados os incidentes de segurança reportados junto ao ambiente contratado.

4.4. Encerramento dos Serviços de Monitoração Remota da Segurança

4.4.1. Quando do encerramento da prestação do serviço de monitoração remota da segurança, a **CONTRATADA** retirará os componentes da solução.

4.4.2. Todas as informações de customização, políticas e regras, logs de auditoria serão disponibilizadas para a **CONTRATANTE** e, em seguida, eliminadas da base de dados da **CONTRATADA**.

4.5. Confidencialidade da Informação.

4.5.1. Todas as informações que trafegam nos equipamentos, bem como todas e quaisquer informações originadas pela **CONTRATANTE**, que a **CONTRATADA** venha a ter acesso serão consideradas “Informações Confidenciais”.

4.5.2. A **CONTRATADA** se compromete a guardar confidencialidade e a não utilizar qualquer tipo de Informação Confidencial para propósitos estranhos àqueles definidos neste Termo de Referência ou em benefício próprio ou de terceiros.

4.5.3. A **CONTRATADA** se compromete a adotar as medidas necessárias para que seus dirigentes, empregados, e em geral todas as pessoas que trabalham sob sua responsabilidade, que precisem conhecer a Informação Confidencial, mantenham a confidencialidade acordada neste instrumento, sendo responsável pela ruptura do compromisso de confidencialidade pelos seus empregados.

4.5.4. A **CONTRATADA** se obriga a devolver ou destruir imediatamente todo o material que contenha Informações Confidenciais, tão logo ocorra a rescisão ou término da vigência do contrato firmado entre as partes.

4.5.5. A **CONTRATANTE** também se compromete a tratar como confidenciais todas as informações de propriedade da **CONTRATADA**, que vier a ter conhecimento, durante a vigência do contrato.

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

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

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

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

5.1.2. Abaixo os tempos de atendimento:

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

5.1.3. SLO de Solicitações e Consultas:

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

ESPECIFICAÇÕES TECNICAS DA SOLUÇÃO

SOLUÇÃO DE SEGURANÇA DE REDE

Solução 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, sendo fornecida em hardware específico.

O hardware e o software fornecidos não podem constar, no momento da apresentação da proposta, em listas de *end-of-sale, end-of-support, end-of-engineering-support* ou *end-of-life* do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante.

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

Item	Descrição	Quantidade
HARDWARE DE FIREWALL		
1	Cluster de Firewall **UTM/NGFW**	1 unidade
SOFTWARE FIREWALL		
2	Pacote de licenças de NG Firewall, IPS/IDS, Controle de Aplicação, Filtro de URL, Anti-vírus, Anti-Malware.	1 unidade

6. ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO

6.1. A performance de todos os serviços ativos de Threat Prevention, deverá ser de 1.5Gbps ou superior.

6.2. Performance de Inspeção de tráfego criptografado (SSL) de no mínimo 290 Mbps, o throughput devem ser comprovados por documento de domínio público do fabricante.

6.3. Performance de IPS de 1.4Gbps ou superior;

6.4. Suporte a, no mínimo, 1.000.000 de conexões do tipo SPI simultâneas;

6.5. Suporte a, no mínimo, 14.000 novas conexões por segundo;

6.6. Disco interno SSD para armazenamento de no mínimo 16 Gb;

6.7. Deve suportar fonte de alimentação interna redundante com chaveamento automático de 100-240 VAC;

6.8. Deverá possuir 4 interfaces de 1GbE SFP;

6.9. 12 interfaces de rede 10/100/1000 base-TX. Todas as interfaces devem possuir mecanismo de auto-sense e seleção de modo half/full duplex.

6.10. As interfaces devem suportar as seguintes atrubuições:

6.10.1. Segmento Wan ou externo;

6.10.2. Segmento WAN, secundário com possibilidade de ativação de recurso para redundância de WAN com balanceamento de carga e WAN Failover por aplicação. O equipamento deverá suportar no mínimo balanceamento de 4 links utilizando diferentes métricas pré-definidas pelo sistema e configuráveis pelo administrador.

6.10.3. Segmento LAN ou rede interna.

6.10.4. Segmento LAN ou rede interna podendo ser configurado como DMZ (Zona desmilitarizada)

6.10.5. Segmento LAN ou rede interna ou Porta de sincronismo para funcionamento em alta disponibilidade

6.10.6. Segmento ou Zona exclusiva para controle de dispositivos Wireless dedicado, com controle e configuração destes dispositivos.

6.10.7. 01 (uma) interface do tipo console ou similar;

6.10.8. 01 (uma) interface de rede dedicada para gerenciamento;

6.11. A VPN Client-to-Site IPsec deve ser licenciada para, no mínimo, 50 usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para no mínimo, 1000 usuários simultâneos, com aquisição de licença futura;

6.12. A VPN SSL deve ser licenciada para, no mínimo, 2 usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para no mínimo, 500 usuários simultâneos, com aquisição de licença futura;

6.13. Suportar 1000 túneis de VPN IPSEC simultâneos;

6.14. Suportar, no mínimo, 1.4Gbps de throughput de VPN IPSEC

6.15. Em appliance com no máximo 2U de altura, com kit de montagem em rack de 19".

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

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

6.18. 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

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

6.20. Possuir redundância do sistema de refrigeração do produto (ventoinha).

7. CARACTERÍSTICAS GERAIS PARA SOLUÇÃO DE FIREWALL

7.1. Todas as funcionalidades descritas devem funcionar no mesmo appliance sem a necessidade de composição de um ou mais produtos;

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

7.3. O hardware e software que executem as funcionalidades de proteção de rede devem ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;

7.4. O equipamento deverá ser baseado em hardware desenvolvido com está finalidade, ou seja, não sendo aceita soluções baseadas em plataforma PC ou equivalente;

7.5. Não serão permitidas soluções baseadas em sistemas operacionais abertos (OpenSource) como Free BSD, Debian ou mesmo Linux;

7.6. Todo o ambiente deverá ser gerenciado através de uma única interface sem a necessidade de produtos de terceiros para compor a solução;

7.7. Deve ser possível suportar arquitetura de armazenamento de logs redundante, permitindo a configuração de equipamentos distintos;

7.8. A solução deverá suportar monitoramento através de SNMP v2 e v3;

7.9. Deve oferecer as funcionalidades de backup/restore tanto da configuração quanto do firmware/sistema operacional através da interface gráfica, assim como permitir ao administrador agendar procedimentos de backups da configuração em determinado dia e hora. O appliance deve armazenar no mínimo 02 (duas) versões distintas do sistema operacional, sendo possível escolher qual versão será inicalizada;de backups da configuração em determinado dia e hora;

7.10. Deve oferecer a funcionalidade de seleção da velocidade da “Porta” a ser realizada preferencialmente através da interface gráfica de gerenciamento. As interfaces devem suportar obrigatoriamente as seguintes atribuições:

- Segmento WAN, ou externo.
- Segmento WAN, secundário com possibilidade de ativação de recurso para redundância de WAN com balanceamento de carga e WAN Failover por aplicação. O equipamento deverá suportar no mínimo balanceamento de 4 links utilizando diferentes métricas pré-definidas pelo sistema e configuráveis pelo administrador.
- Segmento LAN ou rede interna.
- Segmento LAN ou rede interna podendo ser configurado como DMZ (Zona desmilitarizada)
- Segmento LAN ou rede interna ou Porta de sincronismo para funcionamento em alta disponibilidade
- Segmento ou Zona exclusiva para controle de dispositivos Wireless dedicado, com controle e configuração destes dispositivos.

7.11. Suporte a definição de VLAN no firewall, conforme padrão IEEE 802.1q e ser possível criar sub-interfaces lógicas associadas a VLANs e estabelecer regras de filtragem (Stateful Firewall) entre elas;

7.12. A solução deve suportar configuração de link-aggregation de interfaces suportando o protocolo 802.3ad para aumento de throughput.

7.13. A solução deve suportar configuração de port-redundacy de interfaces para a alta disponibilidade de interfaces;

7.14. Os dispositivos de proteção devem ter a capacidade de operar de forma simultânea mediante o uso de suas interfaces físicas nos seguintes modos:

7.15. Modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3);

7.16. Modo sniffer, para inspeção via porta espelhada do tráfego de dados da rede;

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

7.18. 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;

7.19. Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas.

7.20. Possuir DHCP Server interno;

7.21. Suporte a encaminhamento de pacotes UDPs multicast/broadcast entre diferentes interfaces e zonas de segurança como como DHCP Relay, suportando os protocolos e portas:

- Time service—UDP porta 37
- DNS—UDP porta 53
- DHCP—UDP portas 67 e 68
- Net-Bios DNS—UDP porta 137
- Net-Bios Datagram—UDP porta 138
- Wake On LAN—UDP porta 7 e 9
- mDNS—UDP porta 5353
- Suporte a Jumbo Frames;
- Implementar sub-interfaces ethernet lógicas;
- Deve suportar os seguintes tipos de NAT:
- Nat dinâmico (Many-to-1);
- Nat dinâmico (Many-to-Many);
- Nat estático (1-to-1);
- NAT estático (Many-to-Many);
- Nat estático bidirecional 1-to-1;
- Tradução de porta (PAT);
- NAT de origem;
- NAT de destino;

7.22. Suportar NAT de origem e NAT de destino simultaneamente;

7.23. Prover mecanismo contra ataques de falsificação de endereços (IP Spoofing);

7.24. Implementar mecanismo de sincronismo de horário através do protocolo NTP. Para tanto o appliance deve realizar a pesquisa em pelo menos 03 servidores NTP distintos, com a configuração do tempo do intervalo de pesquisa;

7.25. Possuir gerenciamento de tráfego de entrada ou saida, por serviços, endereços IP e regra de firewall, permitindo definir banda mínima garantida e máxima permitida em porcentagem (%) para cada regra definida;

7.26. Implementar 802.1p e classe de serviços CoS (Class of Service) de DSCP (Differentiated Services Code Points);

7.27. Permitir remarcação de pacotes utilizando TOS e/ou DSCP;

7.28. Suporte a policy based routing (PBR), com a capacidade de roteamento por endereço de origem, endereço de destino, serviço, interface ou todas as opções simultâneas;

7.29. Suportar protocolos de roteamento RIP, RIPng, OSPF, OSPFv3 e BGP;

7.30. Suportar Equal Cost Multi-Path (ECMP);

7.31. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);

7.32. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3, RIPng);

7.33. A solução deve suportar integralmente o padrão IPv6, assim como criação de regras com objetos que utilizem endereços IPv4 e IPv6;

7.34. Deve suportar no mínimo as seguintes funcionalidades ou protocolos para o padrão de endereçamento IPv6: Tunel 6 to 4, regras de acesso, objetos de enderço, limitador de conexões IPv6, monitor de conexões, DHCP, gerenciamento HTTPS via IPv6, NAT IPv6, proteção contra ataques to tipo IP Spoofing para IPv6, captura de pacotes IPv6, interface VLAN com endereço IPv6, VPN SSL com o uso do IPv6, controle de URL, Anti-Malware e anti-virus, controle de aplicação, IPS, IKEv2, ICMP6, SNMP, alta disponibilidade, RFC 1981 Path MTU Discovery for IPv6, RFC 2460 IPv6 specification, RFC 2464 Transmission of IPv6 Packets over Ethernet Networks;

7.35. Possui suporte a log via syslog;

7.36. Possuir mecanismo para possibilitar a aplicação de correções e atualizações para o firewall remotamente através da interface gráfica;

7.37. Permitir a visualização em tempo real de todas as conexões TCP e sessões UDP que se encontrem ativas através do firewall;

7.38. Permitir a geração de gráficos em tempo real, representando os serviços mais utilizados e as máquinas mais acessadas em um dado momento;

7.39. Permitir a visualização de estatísticas do uso de CPU do appliance o através da interface gráfica remota em tempo real;

7.40. A solução deverá suportar a tecnologia de SD-WAN e deverá ter no mínimo as seguintes funcionalidades:

- Capacidade de criar um overlay virtual de roteamento, de forma agnóstica a infraestrutura de rede já existente, com a combinação de quaisquer tipos de circuitos WAN;
- Capacidade de agregar no mínimo 3 (três) circuitos WAN distintos em um único canal lógico;
- Implementar segurança fim-a-fim usando solução de criptografia que de maneira automática forneça proteção à redes WANs privadas que transitam por redes públicas compartilhadas;
- Suportar e implementar QoS com classificação, marcação e priorização de tráfego com base em endereço IP de origem/destino, portas TCP/UDP de origem e destino, DSCP (Differentiated Services Code Point), tipo de aplicação camada 7 e traffic shaping nas interfaces;
- Capacidade de realizar a saída local de internet para alguns tráfegos selecionados a partir, no mínimo, dos parâmetros de IP, porta e URL;

- Controle de caminho automático baseado em políticas, com habilidade de selecionar o caminho, no mínimo, através dos seguintes parâmetros simultâneos ou não:
    - ✓ tipo de aplicação;
    - ✓ prioridade de negócio;
    - ✓ latência;
    - ✓ jitter;
    - ✓ perda de pacotes;
    - ✓ A comutação dos caminhos deve ocorrer de maneira dinâmica e automática baseada nas políticas previamente aplicadas;
    - ✓ Permitir a alteração da política de encaminhamento sem impacto no tráfego;
    - ✓ Implementar tecnologia de reconhecimento de aplicações conhecidas (DPI), como Office 365, Facebook e Youtube, como também subaplicações associadas como Facebook Messenger e Office 365 Outlook.

ALTA DISPONIBILIDADE

7.41. A solução deve ser entregue operando em alta disponibilidade no modo Ativo/Standby, com as implementações de Failover;

7.42. Não serão permitidas soluções de cluster (HA) que façam com que o equipamento (s) reinicie após qualquer modificação de parâmetro/configuração seja realizada pelo administrador;

7.43. A solução deve ter capacidade de fazer monitoramento físico das interfaces dos membros do cluster;

7.44. A solução deve operar em alta disponibilidade implementando monitoramento logico de um host na rede, para verificar a existência de problemas lógicos na rede e possibilitar failover;

7.45. A solução deve permitir o uso de endereço MAC virtual para evitar problemas de expiração de tabela ARP em caso de Failover;

7.46. A solução deve possibilitar a sincronização de todas as configurações realizadas na caixa principal do cluster, incluindo, mas não limitado a objetos, regras, rotas, VPN´s e políticas de segurança;

7.47. A solução deve permitir visualizar no equipamento principal, o status da comunicação entre o peers do cluster, status de sincronização das configurações, status atual equipamento backup;

VPN

7.48. Criptografia 3DES, AES 128 e AES 256;

7.49. Autenticação com MD5, SHA-1, SHA-256 e SHA-384;

7.50. Diffie-Hellman: Grupo 2 (1024 bits), Grupo 5 (1536 bits) e Grupo 14 (2048 bits;

7.51. Algoritmo Internet Key Exchange (IKE);

7.52. Autenticação via certificado IKE PKI;

7.53. Deve possuir interoperabilidade com outros fabricantes de acordo com o padrão IPSEC através de RFC`s;

7.54. A solução deve suportar VPNs L2TP, incluindo suporte para iPhone, Windows phone, Android com suporte a cliente L2TP;

7.55. Solução deve suportar VPNs baseadas em políticas e VPNs baseadas em roteamento estático e dinâmico;

7.56. Suportar políticas de roteamento sobre conexões VPN IPSEC do tipo site-to-site com diferentes métricas e serviços. A rota poderá prover aos usuários diferentes caminhos redundantes sobre todas as conexões VPN IPSEC;

7.57. Solução deve incluir a capacidade de estabelecer VPNs com outros firewalls que utilizam IP públicos dinâmicos;

7.58. Permitir a definição de um gateway redundante para terminação de VPN no caso de queda do circuito primário;

7.59. Permitir que seja criado políticas de roteamentos estáticos utilizando IPs de origem, destino, serviços e a própria VPN como parte encaminhadora deste tráfego sendo este visto pela regra de roteamento, como uma interface simples de rede para encaminhamento do tráfego;

7.60. Suportar a criação de túneis IP sobre IP (IPSEC Tunnel), de modo a possibilitar que duas redes com endereço inválido possam se comunicar através da Internet;

AUTENTICAÇÃO

7.61. Permitir a utilização de LDAP, AD e RADIUS;

7.62. Permitir o cadastro manual dos usuários e grupos diretamente na interface de gerência remota do Firewall, caso onde se dispensa um autenticador remoto para o mesmo;

7.63. Suporte a uma rede com múltiplos domínios, possibilitando a integração em um ambiente onde existas domínios diferentes e totalmente segregados;

7.64. Permitir a integração com qualquer autoridade certificadora emissora de certificados X509 que seguir o padrão de PKI descrito na RFC 2459, inclusive verificando as CRLs emitidas periodicamente pelas autoridades, que devem ser obtidas automaticamente pelo firewall via protocolos HTTP e LDAP;

7.65. Permitir o controle de acesso por usuário, para plataformas Windows Me, NT, 2000, 2000, XP, Windows 7, Windows 8 e Windows 10 de forma transparente, para todos os serviços suportados, de forma que ao efetuar o logon na rede, um determinado usuário tenha seu perfil de acesso automaticamente configurado;

7.66. Permitir a restrição de atribuição de perfil de acesso à usuário ou grupo independente ao endereço IP da máquina que o usuário esteja utilizando;

7.67. Suportar recurso de autenticação única para todo o ambiente de rede, ou seja, utilizando a plataforma de autenticação atual que pode ser de LDAP ou AD; o perfil de cada usuário

deverá ser obtido automaticamente através de regras no Firewall DPI (Deep Packet Inspection) sem a necessidade de uma nova autenticação como por exemplo, para os serviços de navegação a Internet atuando assim de forma toda transparente ao usuário. Serviços como HTTP, HTTPS devem apenas consultar uma base de dados de usuários e grupos de servidores 2008/2012 com AD;

IPS

7.68. Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS integrados no próprio appliance de firewall, onde sua console de gerência deverá residir na mesma console centralizada dos appliances de segurança, com suporte a pelo menos 3.000 assinaturas;

7.69. A solução de IPS deverá possuir os seguintes mecanismos de detecção: assinaturas e trabalhar em conjunto com o controle de aplicações;

7.70. A solução de IPS deve fazer a inspeção de todo o pacote, independentemente do tamanho;

7.71. A solução de IPS deve fazer a inspeção de todo o tráfego de forma bidirecional, analisando qualquer tamanho de pacote sem degradar a performance do equipamento solicitada neste edital;

7.72. Possuir capacidade de remontagem de pacotes para identificação de ataques;

7.73. O mecanismo de inspeção deve receber e implementar em tempo real atualizações para os ataques emergentes sem a necessidade de reiniciar o appliance;

7.74. Para cada proteção de segurança, deve ser possível consultar informações no site do fabricante;

7.75. A ferramenta de log deve possuir a capacidade de criar uma regra de exceção a partir do log visualizado na gerência centralizada;

7.76. As regras de exceção devem possuir: origem, destino e serviço;

7.77. A solução deve ser capaz de inspecionar tráfego HTTPS;

7.78. Deverá possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep;

7.79. Detecção de anomalias;

7.80. A solução de IPS deve possuir política capaz de definir o modo de operação (bloqueio ou detecção);

7.81. O módulo de IPS deve possuir assinaturas voltadas para ambientes de servidores de SMTP, Web e DNS;

7.82. O mecanismo de inspeção deve receber e implementar em tempo real atualizações de novas assinaturas sem a necessidade de reiniciar o appliance;

7.83. Para cada proteção, ou para todas as proteções suportadas, deve incluir a opção de adicionar exceções baseado na origem e destino;

7.84. A solução deve ser capaz de detectar e bloquear ataques nas camadas de rede e aplicação, protegendo pelo menos os seguintes serviços: Aplicações web, serviços de e-mail, DNS, FTP, SQL Injection, ataques a sistemas operacionais e VOIP;

7.85. Deve incluir proteção contra worms;

7.86. Deve incluir uma tela de visualização situacional a fim de monitorar graficamente a quantidade de alertas de diferentes severidades e a evolução ao logo do tempo dispondo o sumario quantitativo das ameaças analisadas.

7.87. A solução deve possuir esquema de atualização de assinaturas através de um click;

7.88. Atualização de modo offline, onde poder ser baixado na base do fabricante e posteriormente fazer o upload do arquivo na solução;

7.89. A solução deve suportar importar certificados de servidor para inspeções de tráfego seguro HTTP (HTTPS) de entrada. Depois de importar esses certificados, a solução deve permitir o IPS para Inspeção segura HTTP(HTTPS);

7.90. A solução deverá ser capaz de inspecionar e proteger apenas hosts internos;

7.91. A solução deverá possuir a opção de proteções para sistemas SCADA;

7.92. Solução deverá permitir que o administrador bloqueie facilmente o tráfego de entrada e/ou saída com base em países, sem a necessidade de gerir manualmente os ranges de endereços IP dos países que deseja bloquear.

CONTROLE DE APLICAÇÃO

7.93. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades abaixo:

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

7.95. Capacidade para realizar filtragens/inspeções dentro de portas TCP conhecidas por exemplo porta 80 http, buscando por aplicações que potencialmente expõe o ambiente como: P2P, Kazaa, Morpheus, BitTorrent ou messengers;

7.96. Controlar o uso dos serviços de Instant Messengers como MSN, YAHOO, Google Talk, ICQ, de acordo com o perfil de cada usuário ou grupo de usuários, de modo a definir, para cada perfil, se ele pode ou não realizar download e/ou upload de arquivos, limitar as extensões dos arquivos que podem ser enviados/recebidos e permissões e bloqueio de sua utilização baseados em horários pré-determinados pelo administrador será obrigatório para este item.

7.97. Deverá controlar software FreeProxy tais como ToR, Ultrasurf, Freegate,etc;

7.98. Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;

7.99. Deverá permitir a criação de regras para acesso/bloqueio por subrede de origem e destino;

7.100. Atualizar a base de assinaturas de aplicações automaticamente;

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

7.102. A solução de controle de aplicação WEB deve criar regras granulares possibilitando adicionar tipos de aplicação WEB e categorias por regra, sendo assim criando controle granular de qualquer tipo de acesso não permitido pela empresa;

7.103. Deve implementar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e protocolos;

7.104. Caso a solução não tenha assinaturas pré-definida na solução a mesma deverá possibilitar a criação ou importação de assinaturas personalizadas para os seguintes tipos ou protocolos: HTTP, FTP, E-mail e extensão de arquivos;

7.105. O administrador deve ser capaz de configurar quais comandos FTP são aceitos e quais são bloqueados a partir de comandos FTP pré-definidos;

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

7.107. Deverá possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, uTorrent, etc.) possuindo granularidade de controle/políticas para os mesmos;

7.108. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Facebook e bloquear chat;

7.109. Deverá possibilitar a diferenciação de aplicações Proxies possuindo granularidade de controle/políticas para os mesmos;

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

- Nível de risco da aplicação.
- Categoria de aplicações.

FILTRO DE URL

7.111. Para prover maior visibilidade e controle dos acessos dos usuários do ambiente, deve ser incluído um módulo de filtro de URL integrado no firewall;

7.112. Possuir base contendo no mínimo 20 milhões de sites internet web já registrados e classificados com atualização automática;

7.113. Implementar filtro de conteúdo transparente para o protocolo HTTP, de forma a dispensar a configuração dos browsers das máquinas clientes.

7.114. A plataforma de proteção deve possuir as seguintes funcionalidades de filtro de URL:

7.115. Permitir a criação de listas personalizadas de URLs permitidas e bloqueadas (lista branca e lista negra) ;

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

7.117. Deve ser possível à criação de políticas por usuários, grupos de usuários, IP´s, redes e grupos de redes;

7.118. O mecanismo de Controle de aplicação Web/URL deve apresentar contagem de utilização de regra de acordo com a utilização (hit count);

7.119. Deverá permitir criar política de confirmação de acesso;

7.120. Deve possibilitar a inspeção de tráfego HTTPS (Inbound/Outbound), sendo que para a opção de Outbound não será necessário efetuar o "man-inthe- middle", ou seja, a solução deverá prover mecanismo que irá analisar a conexão HTTPS para verificar se a URL solicitada está na lista de permissões de acesso, de acordo com a política configurada;

7.121. O administrador poderá adicionar filtros por palavra-chave de modo específico;

7.122. Deverá permitir o bloqueio Web através de senha pré configurada pelo administrador

7.123. Deverá 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);

7.124. A solução deve fornecer um mecanismo para solicitação de categorização de URL caso esta não esteja categorizada ou categorizada incorretamente;

7.125. Suportar recurso de autenticação única para todo o ambiente de rede, ou seja, utilizando a plataforma de autenticação atual que pode ser de LDAP ou AD; o perfil de cada usuário deverá ser obtido automaticamente para o controle das políticas de Filtro de Conteúdo sem a necessidade de uma nova autenticação;

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

7.127. Suportar base ou cache de URLs local no appliance ou possibilitar a replicação da base de conhecimento de URLs do fabricante via instalação de máquina virtual, a infraestrutura da máquina virtual (VM) para uso desse recurso será fornecida pelo CONTRATANTE, evitando delay de comunicação/validação das URLs;

7.128. Possuir pelo menos 50 categorias de URLs;

7.129. Suporta a criação de categorias de URLs customizadas;

7.130. Suporta a exclusão de URLs do bloqueio, por categoria;

7.131. Deverá possibilitar a categorização ou recategorização de URL caso não esteja categorizada ou categorizada incorretamente;

7.132. A solução deverá permitir um mecanismo que permita sobrescrever as categorias de URL;

7.133. Permite a customização de página de bloqueio;

PROTEÇÃO CONTRA VIRUS E BOT-NETS

7.134. Deve possuir módulo de antivírus e anti-bot integrado no próprio appliance de segurança;

7.135. A solução de anti-virus integrada deve ter capacidade de analisar arquivos maiores que 1Gbps;

7.136. A solução deve possuir nuvem de inteligência proprietária do fabricante onde seja responsável em atualizar toda a base de segurança dos appliances através de assinaturas;

7.137. Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e qualquer outro mecanismo de redirecionamento de tráfego;

7.138. Implementar funcionalidade de detecção e bloqueio de callbacks;

7.139. A solução deverá ser capaz de detectar e bloquear comportamento suspeito ou anormal da rede;

7.140. A solução Antibot deve possuir mecanismo de detecção que inclui, reputação de endereço IP;

7.141. Implementar interface gráfica WEB segura, utilizando o protocolo HTTPS.

7.142. Implementar interface CLI segura através do protocolo SSH;

7.143. Possuir antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, IMAP, POP3, FTP, CIFS e TCP Stream;

7.144. A solução deve permitir criar regras de exceção de acordo com a proteção;

7.145. Deve possuir visualização na própria interface de gerenciamento referente aos top incidentes através de hosts ou incidentes referentes a incidentes de vírus e Bots;

7.146. Permitir o bloqueio de malwares (vírus, worms, spyware e etc);

7.147. A solução deve ser capaz de proteger contra ataques para DNS;

7.148. A solução deverá ser gerenciada a partir de uma console centralizada com políticas granulares

7.149. A solução deve ser capaz de prevenir acesso a websites maliciosos;

7.150. A solução deve ser capaz de realizar inspeção de tráfego SSL e SSH;

7.151. A solução deverá receber atualizações de um serviço baseado em cloud;

7.152. A solução deverá ser capaz de bloquear a entrada de arquivos maliciosos;

7.153. A solução Antivírus deverá suportar análise de arquivos que trafegam dentro do protocolo CIFS.

7.154. A solução deve suportar funcionalidade de GeoIP, ou seja, a capacidade de identificar, isolar e controlar tráfego baseado na localização (origem e/ou destino), incluindo a capacidade de configuração de listas customizadas para esta mesma finalidade;

PROTEÇÃO CONTRA ATAQUES AVANÇADOS

7.155. A solução deverá prover as funcionalidades de inspeção de tráfego de entrada e saída de malwares não conhecidos ou do tipo APT com filtro de ameaças avançadas e análise de execução em tempo real, e inspeção de tráfego de saída de callbacks;

7.156. Suportar os protocolos HTTP assim como inspeção de tráfego criptografado através de HTTPS e TLS;

7.157. A solução deve ser capaz de inspecionar o tráfego criptografado SSL e SSH;

7.158. Identificar e bloquear a existência de malware em comunicações de entrada e saída, incluindo destinos de servidores do tipo Comando e Controle;

7.159. Implementar mecanismo de bloqueio de vazamento não intencional de dados oriundos de máquinas existentes no ambiente LAN em tempo real;

7.160. Implementar detecção e bloqueio imediato de malwares que utilizem mecanismo de exploração em arquivos no formato PDF, sendo que a solução deve inspecionar arquivo PDF com até 10Mb;

7.161. Implementar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows e Android;

7.162. Conter ameaças de dia zero permitindo ao usuário final o recebimento dos arquivos livres de malware;

7.163. A tecnologia de máquina virtual deverá suportar diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso sem utilização de assinaturas;

7.164. A solução deve possuir nuvem de inteligência proprietária do fabricante onde seja responsável em atualizar toda a base de segurança dos appliance através de assinaturas;

7.165. Implementar a visualização dos resultados das análises de malwares de dia zero nos diferentes sistemas operacionais dos ambientes controlados (sandbox) suportados;

7.166. Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e qualquer outro mecanismo de redirecionamento de tráfego;

7.167. Conter ameaças avançadas de dia zero;

7.168. Toda análise deverá ser realizada de forma automatizada sem a necessidade de criação de regras específicas e/ou interação de um operador;

7.169. Implementar mecanismo do tipo múltiplas fases para verificação de malware e/ou códigos maliciosos;

7.170. Toda a análise e bloqueio de malwares e/ou códigos maliciosos deve ocorrer em tempo real. Não serão aceitas soluções que apenas detectam o malware e/ou códigos maliciosos;

7.171. Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx) e Android APKs no ambiente controlado;

7.172. Implementar a análise de arquivos executáveis, DLLs e ZIP em SSL no ambiente controlado;

7.173. Possuir antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, POP3, FTP, IMAP e CIFS;

7.174. Conter ameaças de dia zero de forma transparente para o usuário final;

7.175. Conter ameaças de dia zero através de tecnologias em nível de emulação e código de registro;

7.176. Implementar mecanismo de pesquisa por diferentes intervalos de tempo;

7.177. Conter ameaças de dia zero via tráfego de internet;

7.178. Permitir a contenção de ameaças de dia zero sem a alteração da infraestrutura de segurança;

7.179. Conter ameaças de dia zero que possam burlar o sistema operacional emulado;

7.180. A solução deve permitir a criação de White list baseado no MD5 do arquivo;

7.181. Conter ameaças de dia zero antes da execução e evasão de qualquer código malicioso;

7.182. Conter exploits avançados;

7.183. A análise “In Cloud” ou local deve prover informações sobre as ações do Malware na máquina infectada, informações sobre quais aplicações são utilizadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo Malware, gerar assinaturas de Antivírus e Antispyware automaticamente, definir URLs não confiáveis utilizadas pelo novo Malware e prover Informações sobre o usuário infectado (seu endereço IP e seu login de rede);

7.184. Suporte a submissão manual de arquivos para análise através do serviço de Sandbox;

ADMINISTRAÇÃO

7.185. Suportar políticas baseadas por grupos de usuários deverão ser suportadas pelo dispositivo.

7.186. Permitir a criação de perfis de administração distintos, de forma a possibilitar a definição de diversos administradores para o firewall, cada um responsável por determinadas tarefas da administração;

7.187. Fornecer gerência remota, com interface gráfica nativa;

7.188. A interface gráfica deverá possuir assistentes para facilitar a configuração inicial e a realização das tarefas mais comuns na administração do firewall, incluindo a configuração de VPN IPSECs, NAT, perfis de acesso e regras de filtragem;

7.189. Possuir mecanismo que permita a realização de cópias de segurança (backups) e sua posterior restauração remotamente, através da interface gráfica, sem necessidade de se reinicializar o sistema;

7.190. Possuir mecanismo para possibilitar a aplicação de correções e atualizações para o firewall remotamente através da interface gráfica;

7.191. Permitir a visualização em tempo real de todas as conexões TCP e sessões UDP que se encontrem ativas através do firewall e a remoção de qualquer uma destas sessões ou conexões;

7.192. Permitir a geração de gráficos em tempo real, representando os serviços mais utilizados e as máquinas mais acessadas em um dado momento;

7.193. Permitir a visualização de estatísticas do uso de CPU, memória da máquina onde o firewall está rodando e tráfego de rede em todas as interfaces do Firewall através da interface gráfica remota, em tempo real e em forma tabular e gráfica;

7.194. Permitir a conexão simultânea de vários administradores, sendo um deles com poderes de alteração de configurações e os demais apenas de visualização das mesmas. Permitir que o segundo ao se conectar possa enviar uma mensagem ao primeiro através da interface de administração.

7.195. Possibilitar o registro de toda a comunicação realizada através do firewall, e de todas as tentativas de abertura de sessões ou conexões que forem recusadas pelo mesmo;

7.196. Possuir interface orientada a linha de comando para a administração do firewall a partir do console ou conexão SSH sendo está múltiplas sessões simultâneas.

7.197. Possuir mecanismo que permita inspecionar o tráfego de rede em tempo real (sniffer) via interface gráfica, podendo opcionalmente exportar os dados visualizados para arquivo formato PCAP e permitindo a filtragem dos pacotes por protocolo, endereço IP origem e/ou destino e porta IP origem e/ou destino, usando uma linguagem textual;

7.198. Permitir a visualização do tráfego de rede em tempo real tanto nas interfaces de rede do Firewall quando nos pontos internos do mesmo: anterior e posterior à filtragem de pacotes, onde o efeito do NAT (tradução de endereços) é eliminado;

7.199. Possuir sistema de respostas automáticas que possibilite alertar imediatamente o administrador através de e-mails, janelas de alerta na interface gráfica, execução de programas e envio de Traps SNMP;

RELATÓRIOS

7.200. Ser capaz de visualizar, de forma direta no appliance e em tempo real, as aplicações mais utilizadas, os usuários que mais estão utilizando estes recursos informando sua sessão, total de pacotes enviados, total de bytes enviados e média de utilização em Kbps, URLs acessadas e ameaças identificadas.

7.201. Possibilitar a geração de pelo menos os seguintes tipos de relatório com cruzamento de informações, mostrados em formato HTML: máquinas acessadas X serviços bloqueados, usuários X URLs acessadas, usuários X categorias Web bloqueadas (em caso de utilização de um filtro de conteúdo Web);

7.202. Possibilitar a geração de pelo menos os seguintes tipos de relatório, mostrados em formato HTML: máquinas mais acessadas, serviços mais utilizados, usuários que mais utilizaram serviços, URLs mais visualizadas, ou categorias Web mais acessadas (em caso de existência de um filtro de conteúdo Web), maiores emissores e receptores de e-mail;

7.203. Permitir o envio dos relatórios, através de e-mail para usuários pré-definidos;

7.204. Possuir relatórios pré-definidos na solução e permitir a criação de relatórios customizados;

7.205. Possibilitar a geração dos relatórios sob demanda e através de agendamento diário, semanal e mensal. No caso de agendamento, os relatórios deverão ser publicados de forma automática

7.206. Disponibilizar download dos relatórios gerados;

8. Garantia, Suporte e Licenciamento

8.1. Deve contemplar suporte do Fabricante pelo período vigente ao contrato.

8.2. O suporte do fabricante deve ter um sistema de abertura de chamados para acompanhamento – funcionando 24 horas por dia e 7 dias por semana. Para atendimento telefônico, deve operar em língua Portuguesa pelo menos em regime 8x5.

8.3. Deve assegurar a utilização de novas versões de software da solução sem ônus a CONTRATANTE, sempre que esta estiver disponível oficialmente.

9. Conformidade

9.1. O Fabricante deve comprovar participação no MAPP da Microsoft;

9.2. A tecnologia deve possuir pelo menos uma certificação da ICSA Labs, ICSA Firewall ou Antivírus;

9.3. O fabricante da solução deverá ser avaliado pela NSS Labs (Network Security Services) no desempenho do Next Generation Firewall Comparative Analysis mais recente, estando no “Security Value Map” acima de 90 % (noventa por cento) da avaliação de segurança efetiva.

9.4. O fornecimento dos produtos e seus licenciamentos devem ser entregues através de empresa credenciada e autorizada pelo fabricante. Isto deve ser comprovada através de carta de reconhecimento assinada pelo representante legal do fabricante no Brasil

9.5. Deve ser homologado pela ANATEL.

TABELA DE ENDEREÇOS – ANEXO II

LINHAS ANALOGICAS: TABELA 1

SERVIÇO	Classe de Serviço	Núm. Linha	Endereço	CEP	Município	UF
TERMINAL	LINA	1434782135	R BARROSO,ALM, 75	17690000	BASTOS	SP
TERMINAL	LINA	1434782148	R PEDRO I,DOM, 19	17690000	BASTOS	SP
TERMINAL	LINA	1434782609	R CAXIAS,DQ, 600	17690000	BASTOS	SP
TERMINAL	LINA	1434781955	R RUI BARBOSA, 1217	17690000	BASTOS	SP
TERMINAL	LINA	1434781821	AV GASPAR RICARDO, 1800	17690000	BASTOS	SP
TERMINAL	LINA	1434782096	R UNIAO, SN	17690000	BASTOS	SP
TERMINAL	LINA	1434786814	AV DEZOITO DE JUNHO, 175	17690000	BASTOS	SP
TERMINAL	LINA	1434783103	R AMAZONAS, 65	17690000	BASTOS	SP
TERMINAL	LINA	1434784005	R VARGAS,PRES, 488	17690000	BASTOS	SP
TERMINAL	LINA	1434782740	R EMILIO MONTEIRO, 246	17690000	BASTOS	SP
TERMINAL	LINA	1434783554	R FLORIANO PEIXOTO,MAL, 545	17690000	BASTOS	SP
TERMINAL	LINA	1434783237	R SATOSHI NAGAHASHI, 800	17690000	BASTOS	SP
TERMINAL	LINA	1434782281	R OSORIO,GAL, 1006	17690000	BASTOS	SP
TERMINAL	LINA	1434782507	R FLORIANO PEIXOTO,MAL, 790	17690000	BASTOS	SP
TERMINAL	LINA	1434781059	AV DEZOITO DE JUNHO, 461	17690000	BASTOS	SP
TERMINAL	LINA	1434781115	R CAXIAS,DQ, 600	17690000	BASTOS	SP
TERMINAL	LINA	1434781600	AV DEZOITO DE JUNHO, 335	17690000	BASTOS	SP
TERMINAL	LINA	1434784515	R ADHEMAR DE BARROS, 800	17690000	BASTOS	SP
TERMINAL	LINA	1434781608	R OSVALDO CRUZ, 878	17690000	BASTOS	SP
TERMINAL	LINA	1434781611	R SENJIRO HATANAKA, 99	17690000	BASTOS	SP
TERMINAL	LINA	1434781621	AV GASPAR RICARDO, 15000	17690000	BASTOS	SP
TERMINAL	LINA	1434782155	R CAMPOS SALLES, 355	17690000	BASTOS	SP
TERMINAL	LINA	1434781650	AV GASPAR RICARDO, 1700	17690000	BASTOS	SP
TERMINAL	LINA	1434781604	R ADHEMAR DE BARROS, 530	17690000	BASTOS	SP
TERMINAL	LINA	1434782066	AV DEZOITO DE JUNHO, 90	17690000	BASTOS	SP
TERMINAL	LINA	1434781200	R TUCANOS, 315	17690000	BASTOS	SP
TERMINAL	LINA	1434781790	AV DEZOITO DE JUNHO, 251	17690000	BASTOS	SP
TERMINAL	LINA	1434782200	AV GASPAR RICARDO, 1800	17690000	BASTOS	SP
TERMINAL	LINA	1434786690	R JOSE CANDIDO MANCILHIA, 125	17690000	BASTOS	SP
TERMINAL	LINA	1434781613	AV GASPAR RICARDO, 1800	17690000	BASTOS	SP
TERMINAL	LINA	1434785066	R SETE DE SETEMBRO, 455	17690000	BASTOS	SP
TERMINAL	LINA	1434783156	AV DEZOITO DE JUNHO, 162	17690000	BASTOS	SP
TERMINAL	LINA	1434782376	R VARGAS,PRES, 1040	17690000	BASTOS	SP
TERMINAL	LINA	1434781331	R AMAZONAS, 65	17690000	BASTOS	SP
TERMINAL	LINA	1434785004	R BRASILIA, 320	17690000	BASTOS	SP
TERMINAL	LINA	1434784007	R BEM TE VI, 165	17690000	BASTOS	SP
TERMINAL	LINA	1434786557	AV GASPAR RICARDO, 757	17690000	BASTOS	SP
TERMINAL	LINA	1434787013	R CIDADE DE KUMANO, 380	17690000	BASTOS	SP
TERMINAL	LINA	1434786941	R OSVALDO CRUZ, 878	17690000	BASTOS	SP
TERMINAL	LINA	1434781438	R BARROSO,ALM, 75	17690000	BASTOS	SP
TERMINAL	LINA	1434786186	R OSORIO,GAL, 894	17690000	BASTOS	SP
TERMINAL	LINA	1434781868	R EMILIO MONTEIRO, 515	17690000	BASTOS	SP
TERMINAL	LINA	1434786169	R SETE DE SETEMBRO, 445	17690000	BASTOS	SP
TERMINAL	LINA	1434782470	R CAXIAS,DQ, 640	17690000	BASTOS	SP
TERMINAL	LINA	1434783307	AV DEZOITO DE JUNHO, 162	17690000	BASTOS	SP
TERMINAL	LINA	1434781322	R VARGAS,PRES, 400	17690000	BASTOS	SP
TERMINAL	LINA	1434781648	R PERNAMBUCO, 100	17690000	BASTOS	SP
TERMINAL	LINA	1434786401	R SETE DE SETEMBRO, 339	17690000	BASTOS	SP
TERMINAL	LINA	1434786449	R BEM TE VI, 25	17690000	BASTOS	SP
TERMINAL	LINA	1434781969	R SETE DE SETEMBRO, 455	17690000	BASTOS	SP

PARECER
Examinado e aprovado pela Secretaria Mun.dos
Negócios Juridicos de acordo com a Lei 8.666/93
Atualizada pela Lei 8.883/94
Bastos-SP, 23 de outubro de 2019
Rafael Teixeira Sebastiani – OAB/SP 355751
Procurador Jurídico

TRONCOS DIGITAIS : TABELA 2

Produto	Canais	Ramais	Núm. Linha	Endereço	CEP	Município	UF
DDR	15	15	1434789800	R ADHEMAR DE BARROS, 530	17690000	BASTOS	SP
DDR	10	10	1434781115	R CAXIAS,DQ, 600	17690000	BASTOS	SP
DDR	10	10	1434786169	R SETE DE SETEMBRO, 445	17690000	BASTOS	SP

ACESSO LINK DEDICADO: TABELA 3

Produto	Velocidade	Qtd. de Acesso Dados	Endereço	CEP	Município	UF
IP DEDICADO	100 MBPS	1	RUA ADHEMAR DE BARROS, 600	17690000	BASTOS	SP

CLÁUSULA SEGUNDA

A CONTRATANTE pagará à CONTRATADA a importância total, **de R$...**, (...),Os pagamentos serão creditados em nome da contratada, mediante ordem bancária em conta corrente por ela indicada ou por meio de ordem bancária para pagamento de faturas com código de barras, uma vez satisfeitas as condições estabelecidas neste contrato, e deverá ser efetivado parceladamente até o 10º dia subsequente de cada mês, após a emissão das Notas Fiscais apresentadas pela CONTRATADA.

CLÁUSULA TERCEIRA

Somente serão aceitos reajustes para Contratos com período de duração igual ou superior a 12 meses, conforme a Lei 10.192/2001.

CLÁUSULA QUARTA

Os encargos sociais, com funcionários, como adicional de insalubridade, periculosidade, horas extras cobradas, ficarão por conta exclusivamente da CONTRATADA, cabendo à CONTRATANTE arcar com as despesas somente dos serviços.

CLÁUSULA QUINTA

A fiscalização do contrato ficará a cargo do responsável do CPD Sr. Leandro Kislek Betetto .

PARECER
Examinado e aprovado pela Secretaria Mun.dos
Negócios Juridicos de acordo com a Lei 8.666/93
Atualizada pela Lei 8.883/94
Bastos-SP, 23 de outubro de 2019
Rafael Teixeira Sebastiani – OAB/SP 355751
Procurador Jurídico

Quando da emissão das Notas Fiscais, as mesmas deverão ser encaminhadas ao funcionário autorizado, para que seja realizada a conferência, somente após carimbada e assinada, será encaminhada ao Setor de Contabilidade para sua Liquidação e posterior pagamento.

CLÁUSULA SEXTA

Para suprir as despesas do presente Contrato, serão utilizadas verbas do exercício de 2019, suplementadas se necessário for:-

Estado de São Paulo
Prefeitura Municipal de Bastos
Órgão 2 - Executivo

Modalidade:	**PREGÃO PRESENCIAL**	**Nº**	**098/19**
Objeto:	Classificação orçamentária com a categoria econômica funcional programática para contratação de empresa no ramo de telefonia fixa destinado a vários setores da municipalidade		

Despesa desdobrada	Natureza da despesa	Nomenclatura da Despesa	Funcional Programática	Unidade Orçamentária	Despesa Principal	Fonte	CA	Saldo da Dotação	Nome do Recurso
6409	33904004	COMUNICAÇÃO DE DADOS	02.01.00.04.122.0003.2.003	GABINETE DO PREFEITO E DEPENDÊNCIAS	621	1	110.0000	3.376,03	TESOURO
6346	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
6410	33904004	COMUNICAÇÃO DE DADOS	02.02.00.04.122.0004.2.004	SEC. MUN. DE ADMINISTRAÇÃO	696	1	110.0000	11.097,89	TESOURO
6347	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
7179	33904004	COMUNICAÇÃO DE DADOS	02.03.00.04.122.0006.2.008	MANUT. SEC. MUN. DE PLANEJAMENTO	2404	1	110.000	1.516,08	TESOURO
6348	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
6477	33904004	COMUNICAÇÃO DE DADOS	02.04.00.12.361.0014.2.014	SEC. MUN. DE EDUCAÇÃO E CULTURA - ENSINO FUNDAMENTAL	2445	1	2200000	9.044,95	TESOURO
6358	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
6478	33904004	COMUNICAÇÃO DE DADOS	02.04.00.12.365.0016.2.016	MANUT. ENSINO INFANTIL - PRÉ-ESCOLA	2446	1	213.0000	20.151,98	TESOURO
6359	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							

PARECER
Examinado e aprovado pela Secretaria Mun.dos
Negócios Juridicos de acordo com a Lei 8.666/93
Atualizada pela Lei 8.883/94
Bastos-SP, 23 de outubro de 2019
Rafael Teixeira Sebastiani – OAB/SP 355751
Procurador Jurídico

6479	33904004	COMUNICAÇÃO DE DADOS	02.04.00.13.391.0027.2.049	MANUT. DO PATRIMÔNIO HISTÓRICO, ARTÍSTICO E ARQUEOLÓGICO	2447	1	110.0000	324,49	TESOURO
6360	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
6489	33904004	COMUNICAÇÃO DE DADOS	02.05.00.10.122.0047.2.074	MANUT. DA SEC. DE SAÚDE	716	1	310.0000	6.736,65	TESOURO
6349	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
6489	33904004	COMUNICAÇÃO DE DADOS	02.05.00.10.301.0037.2.017	MANUT. DO FUNDO MUN. DE SAÚDE	1915	2	300.0056	7.739,03	PAB
6350	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
6789	33904004	COMUNICAÇÃO DE DADOS	02.05.00.10.302.0017.2.120	PRONTO-SOCORRO MUNICIPAL	724	1	310.0000	1.484,94	TESOURO
6351	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
6480	33904004	COMUNICAÇÃO DE DADOS	02.06.00.27.812.0019.2.019	MANUT. DA SEC. MUN. DE ESPORTES	697	1	110.000	2.813,50	TESOURO
6352	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
7178	33904004	COMUNICAÇÃO DE DADOS	02.07.00.04.122.0004.2.020	MANUT. SEC. MUN. DOS NEGÓCIOS JURÍDICOS	1950	1	110.0000	300,00	TESOURO
6353	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
6481	33904004	COMUNICAÇÃO DE DADOS	02.08.00.08.244.0021.2.021	MANUT. SEC. DE PROMOÇÃO SOCIAL	698	1	510.0000	2.565,44	TESOURO
6354	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
6483	33904004	COMUNICAÇÃO DE DADOS	02.09.00.20.606.0026.2.026	MANUT. DA SEC. DE AGRICULTURA E MEIO AMBIENTE	717	1	110.0000	1.534,49	TESOURO
6355	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
6482	33904004	COMUNICAÇÃO DE DADOS	02.11.00.08.243.0024.2.025	MANUT. DO FUNDO MUN. DOS DIRETOS DA CRIANÇA E DO ADOLESCENTE	719	1	500.0003	2.468,41	TESOURO
6356	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
6479	33904004	COMUNICAÇÃO DE DADOS	02.12.00.23.695.0030.2.053	MANUT. DA SEC. DE TURISMO	718	1	110.0000	1.578,36	TESOURO
6357	33904005	SERVIÇOS DE TELEFONIA							

PARECER
Examinado e aprovado pela Secretaria Mun.dos
Negócios Juridicos de acordo com a Lei 8.666/93
Atualizada pela Lei 8.883/94
Bastos-SP, 23 de outubro de 2019
Rafael Teixeira Sebastiani – OAB/SP 355751
Procurador Jurídico

		FIXA E MÓVEL							
Total de dotação disponível nesta data 23/10/2019:								**72.732,24**	

Neusa Kyoka Hitaka Nishida
Assessora Div. Contabilidade
R.G. 18.913.743-5 SSP/SP

Estado de São Paulo
Prefeitura Municipal de Bastos
Órgão 2 - Executivo

Modalidade:	**PREGÃO PRESENCIAL**	**Nº**	**098/19**
Objeto:	Classificação orçamentária com a categoria econômica funcional programática para contratação de empresa no ramo de telefonia fixa destinado a vários setores da municipalidade		

Despesa desdobrada	Natureza da despesa	Nomenclatura da Despesa	Funcional Programática	Unidade Orçamentária	Despesa Principal	Fonte	CA	Saldo da Dotação	Nome do Recurso
	33904004	COMUNICAÇÃO DE DADOS	02.01.00.04.122.0003.2.003	GABINETE DO PREFEITO E DEPENDÊNCIAS	621	1	110.0000	260.000,00	TESOURO
	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
	33904004	COMUNICAÇÃO DE DADOS	02.02.00.04.122.0004.2.004	SEC. MUN. DE ADMINISTRAÇÃO	696	1	110.0000	80.000,00	TESOURO
	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
	33904004	COMUNICAÇÃO DE DADOS	02.02.00.04.124.0004.2.013	MANUTENÇÃO DO CONTROLE INTERNO	729	1	110.0000	11.000,00	TESOURO
	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
	33904004	COMUNICAÇÃO DE DADOS	02.03.00.04.122.0006.2.008	SEC. MUN. DE PLANEJAMENTO	2404	1	110.000	12.000,00	TESOURO
	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
	33904004	COMUNICAÇÃO DE DADOS	02.04.00.12.361.0014.2.014	SEC. MUN. DE EDUCAÇÃO E CULTURA - ENSINO FUNDAMENTAL	2445	1	2200000	110.000,00	TESOURO
	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							

PARECER
Examinado e aprovado pela Secretaria Mun.dos
Negócios Juridicos de acordo com a Lei 8.666/93
Atualizada pela Lei 8.883/94
Bastos-SP, 23 de outubro de 2019
Rafael Teixeira Sebastiani – OAB/SP 355751
Procurador Jurídico

	33904004	COMUNICAÇÃO DE DADOS	02.04.00.12.365.0016.2.016	MANUT. ENSINO INFANTIL - PRÉ-ESCOLA	2446	1	213.0000	70.000,00	TESOURO
	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
	33904004	COMUNICAÇÃO DE DADOS	02.04.00.13.391.0027.2.049	MANUT. DO PATRIMÔNIO HISTÓRICO, ARTÍSTICO E ARQUEOLÓGICO	2447	1	110.0000	7.000,00	TESOURO
	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
	33904004	COMUNICAÇÃO DE DADOS	02.05.00.10.122.0047.2.074	MANUT. DA SEC. DE SAÚDE	716	1	310.0000	120.000,00	TESOURO
	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
	33904004	COMUNICAÇÃO DE DADOS	02.05.00.10.301.0037.2.017	MANUT. DO FUNDO MUN. DE SAÚDE	820	1	310.0000	80.000,00	TESOURO
	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
	33904004	COMUNICAÇÃO DE DADOS	02.05.00.10.301.0037.2.017	MANUT. DO FUNDO MUN. DE SAÚDE	821	5	300.0001	20.000,00	PAB
	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
	33904004	COMUNICAÇÃO DE DADOS	02.05.00.10.301.0037.2.017	MANUT. DO FUNDO MUN. DE SAÚDE	1915	2	300.0056	48.000,00	PAB
	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
	33904004	COMUNICAÇÃO DE DADOS	02.05.00.10.301.0037.2.057	MANUT. DO PROGRAMA SAÚDE DA FAMÍLIA - PSF	822	1	310.000	20.000,00	TESOURO
	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
	33904004	COMUNICAÇÃO DE DADOS	02.05.00.10.301.0037.2.103	MANUTENÇÃO DO CEO	823	1	310.0000	10.000,00	TESOURO
	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
	33904004	COMUNICAÇÃO DE DADOS	02.05.00.10.302.0017.2.120	PRONTO-SOCORRO MUNICIPAL	724	1	310.0000	20.000,00	TESOURO
	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
	33904004	COMUNICAÇÃO DE DADOS	02.05.00.10.302.0038.2.067	TETO ATENÇÃO HOSPITALAR E AMBULATORIAL	827	1	310.0000	10.000,00	TESOURO
	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							

PARECER
Examinado e aprovado pela Secretaria Mun.dos
Negócios Juridicos de acordo com a Lei 8.666/93
Atualizada pela Lei 8.883/94
Bastos-SP, 23 de outubro de 2019
Rafael Teixeira Sebastiani – OAB/SP 355751
Procurador Jurídico

	33904004	COMUNICAÇÃO DE DADOS	02.05.00.10.302.0038.2.142	MANUT. DA REDE DE SAÚDE MENTAL	826	1	310.0000	10.000,00	TESOURO
	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
	33904004	COMUNICAÇÃO DE DADOS	02.05.00.10.304.0032.2.068	MANUT. DA VIGILÂNCIA SANITÁRIA	828	1	310.000	10.000,00	TESOURO
	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
	33904004	COMUNICAÇÃO DE DADOS	02.05.00.10.305.0032.2.018	MANUT. DA VIGILÂNCIA EPIDEMIOLÓGICA	829	1	310.0000	10.000,00	TESOURO
	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
	33904004	COMUNICAÇÃO DE DADOS	02.06.00.27.812.0019.2.019	MANUT. DA SEC. MUN. DE ESPORTES	697	1	110.000	10.000,00	TESOURO
	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
	33904004	COMUNICAÇÃO DE DADOS	02.07.00.04.122.0004.2.020	MANUT. SEC. MUN. DOS NEGÓCIOS JURÍDICOS	1950	1	110.0000	5.000,00	TESOURO
	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
	33904004	COMUNICAÇÃO DE DADOS	02.08.00.08.244.0021.2.021	MANUT. SEC. DE PROMOÇÃO SOCIAL	698	1	510.0000	40.000,00	TESOURO
	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
	33904004	COMUNICAÇÃO DE DADOS	02.09.00.20.606.0026.2.026	MANUT. DA SEC. DE AGRICULTURA E MEIO AMBIENTE	717	1	110.0000	10.000,00	TESOURO
	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
	33904004	COMUNICAÇÃO DE DADOS	02.11.00.08.243.0024.2.025	MANUT. DO FUNDO MUN. DOS DIRETOS DA CRIANÇA E DO ADOLESCENTE	719	1	500.0003	8.000,00	TESOURO
	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
	33904004	COMUNICAÇÃO DE DADOS	02.12.00.23.695.0030.2.053	MANUT. DA SEC. DE TURISMO	718	1	110.0000	20.000,00	TESOURO
	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							
	33904004	COMUNICAÇÃO DE DADOS	02.13.00.04.122.0004.2.082	MANUT. DA SEC. DE FINANÇAS	836	1	110.0000	95.000,00	TESOURO
	33904005	SERVIÇOS DE TELEFONIA FIXA E MÓVEL							

PARECER
Examinado e aprovado pela Secretaria Mun.dos
Negócios Juridicos de acordo com a Lei 8.666/93
Atualizada pela Lei 8.883/94
Bastos-SP, 23 de outubro de 2019
Rafael Teixeira Sebastiani – OAB/SP 355751
Procurador Jurídico

2020								**1.096.000,00**	
Neusa Kyoka Hitaka Nishida Assessora Div. Contabilidade R.G. 18.913.743-5 SSP/SP									

CLÁUSULA SÉTIMA

O presente Contrato iniciar-se-á em ....., tendo o seu término previsto para ..... (12 meses), podendo ser prorrogado por iguais e sucessivos períodos até o limite de 60 meses, sendo que no final do contrato havendo saldo será estornado. Caso termine a quantidade solicitada antes do prazo especificado, será aditado em até 25 (vinte e cinco) por cento, nos termos do art. 65, § 1º, da Lei 8.666/93.

A - CONSTITUI DIREITOS DA CONTRATANTE:-

1º - Alterar o Contrato com as devidas justificativas, nos casos enumerados nos incisos I e II e alíneas deste artigo 65.

2º - O Contratado fica obrigado a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem nas obras, serviços ou compras, até 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.....Art. 65, § 1º.

3º - Em havendo alteração unilateral do contrato que aumente os encargos do contratado, a Administração deverá restabelecer, por aditamento, o equilíbrio econômico-financeiro inicial. Art. 65, § 6º.

4º - Exigir o cumprimento fiel do contrato pelas partes, de acordo com as cláusulas avençadas e as normas desta Lei, respondendo cada uma pelas consequências de sua inexecução total ou parcial. Art. 66.

5º - O direito de acompanhar e fiscalizar por representante da Administração especialmente designado, permitida a contratação de terceiros para assistí-lo e subsidiá-lo de informações pertinentes a essa atribuição. Art. 67.

6º - Obrigar o Contratado a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, o objeto do contrato em que se verificarem vícios defeitos ou incorreções resultantes da execução ou de materiais empregados. Art. 69.

7º - Responsabilizar o Contratado pelos danos causados diretamente à Administração o a terceiros, decorrentes de sua culpa ou dolo na execução do contrato, não excluindo ou reduzindo essa responsabilidade a fiscalização ou o acompanhamento pelo órgão interessado. Art.70.

8º - Responsabilizar o Contratado pelos encargos trabalhistas, previdenciários, fiscais e comerciais resultantes da execução do contrato. (art. 71 "caput"). § 1º - A inadimplência do contratado, com referência aos encargos estabelecidos neste artigo, não transfere à Administração Pública a responsabilidade por seu pagamento, nem poderá onerar o objeto do contrato ou restringir a regularização.

PARECER
Examinado e aprovado pela Secretaria Mun.dos
Negócios Juridicos de acordo com a Lei 8.666/93
Atualizada pela Lei 8.883/94
Bastos-SP, 23 de outubro de 2019
Rafael Teixeira Sebastiani – OAB/SP 355751
Procurador Jurídico

9º - A Administração rejeitará no todo ou em parte, obra, serviço ou fornecimento executado em desacordo com o contrato. Art. 76.

10º - A inexecução total ou parcial do contrato enseja a sua rescisão, com as consequências contratuais e as previstas em lei ou regulamento. Art. 77.

11º - O descumprimento total ou parcial das cláusulas descritas neste contrato, implicará nas consequências previstas no Art. 78 e incisos desta Lei. 8.666/93.

B - CONSTITUI DIREITOS DA CONTRATADA:-

1º - Em caso de rescisão, com base nos incisos XII a XVII do art. 78, sem que haja culpa do contratado, será este ressarcido dos prejuízos regulamentares comprovados que houver sofrido, tendo ainda direito a:-

I - devolução de garantia se for o caso;

II - pagamentos devidos pela execução do contrato até a data da rescisão;

III - pagamento do custo da desmobilização.

2º - Rescindir o contrato, em caso de supressão, por parte da Administração, de obras, serviços ou compras, acarretando modificação do valor inicial do contrato além do limite permitido no § 1º do art. 65 desta Lei.

3º - Suspender o contrato, em caso de atraso de pagamento superior a noventa dias, até que seja normalizada a situação. Art. 79, inc. XV.

4º - Direito a prorrogação do contrato, ocorrendo impedimento, paralisação ou sustação do contrato, o cronograma de execução será prorrogado automaticamente por igual tempo. Art. 79, § 5º.

5º - Direito a indenização no caso de nulidade do contrato, se este houver executado até a data em que ela for declarada e por outros prejuízos regularmente comprovados, contanto que não lhe seja imputável, promovendo-se a responsabilidade de quem lhe deu causa. Art. 59, § único.

CLÁUSULA OITAVA

O proponente consagrado pelo Adjudicatório deverá assinar o Contrato no prazo de 48 horas. Àquele que manifestamente se negar a cumprir sem motivo justo, terá seu Certificado de Registro suspenso pelo período de até dois anos, conforme previsto no Edital, sendo então chamado o segundo classificado e assim sucessivamente. Conforme Art. 78, inciso XII, este Contrato poderá ser rescindido a qualquer tempo, por ato unilateral do Chefe do Executivo, assegurado o contraditório e a ampla defesa.

- SANÇÕES, MULTAS E PENALIDADE PELO INADIMPLEMENTO CONTRATUAL:-

Art. 87 - Pela inexecução total ou parcial do contrato a Administração poderá, garantida a prévia defesa, aplicar ao contratado as seguintes sanções:-

I - Advertência;

II - multa, correspondente a 10% do valor Adjudicado;

III - suspensão temporária de participação em licitação e impedimento de contratar com a Administração, por prazo não superior a 2 (dois) anos; esse período será apurado em processo Administrativo;

IV - Declaração de inidoneidade para licitar ou contratar com a Administração Pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que o contratado ressarcir a Administração pelos prejuízos resultantes e após decorrido o prazo da sanção aplicada com base no inciso anterior.

Parágrafo Terceiro - As sanções previstas nos inciso IV deste artigo é de competência exclusiva do Secretário Municipal de Administração, conforme o caso, facultada a defesa do interessado no respectivo processo, no prazo de l0 (dez) dias da abertura de vista, podendo a reabilitação ser requerido após 2 (dois) anos de sua aplicação.

No caso de inadimplemento das obrigações, as partes elegem desde já o Fôro da Cidade de Bastos, com renúncia expressa a qualquer outro, por mais privilegiado que seja, ***ressalvando desde já os direitos da Administração, previstos no Art. 55, inciso IX, da Lei 8.666/93.***

E por estarem concordes ao presente, mandaram digitar em três vias de igual teor e forma, na presença de duas testemunhas que assinam juntamente com os Contratantes.

PREFEITURA DO MUNICÍPIO DE BASTOS,
aos ...de 2019

MANOEL IRONIDES ROSA
PREFEITO MUNICIPAL
CONTRATANTE

CONTRATADO

TESTEMUNHAS:-

MÁRCIO KOJI NOKAI **ADRIANO RIBEIRO**

PARECER
Examinado e aprovado pela Secretaria Mun.dos
Negócios Juridicos de acordo com a Lei 8.666/93
Atualizada pela Lei 8.883/94
Bastos-SP, 23 de outubro de 2019
Rafael Teixeira Sebastiani – OAB/SP 355751
Procurador Jurídico

ANEXO LC-01 - TERMO DE CIÊNCIA E DE NOTIFICAÇÃO
(Contratos)

CONTRATANTE: PREFEITURA DO MUNICÍPIO DE BASTOS
CONTRATADO:
CONTRATO Nº (DE ORIGEM):.../2018
OBJETO: CONTRATAÇÃO DE EMPRESA ESPECIALIZADA PARA PRESTAÇÃO DE SERVIÇOS DE TELECOMUNICAÇÕES E TECNOLOGIA DA INFORMAÇÃO, SENDO ELES: (1) PRESTAÇÃO DE SERVIÇO DE TELECOMUNICAÇÕES STFC (SERVIÇO TELEFÔNICO FIXO COMUTADO) NAS MODALIDADES ANALÓGICO E DIGITAL, (2) FORNECIMENTO DE LINK DEDICADO DE ACESSO À INTERNET, (3) FORNECIMENTO E IMPLANTAÇÃO DE SOLUÇÃO DE SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO, NOS TERMOS DAS CONCESSÕES OUTORGADAS PELA AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES – ANATEL.
ADVOGADO/ Nº OAB: (*)KLEYTON EDUARDO RODRIGUES SAITO- PROCURADOR JURIDICO – OAB/SP 347876

Pelo presente TERMO, nós, abaixo identificados:

1. Estamos CIENTES de que:

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

2. Damo-nos por NOTIFICADOS para:

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

LOCAL e DATA: BASTOS, ... DE ... DE 2019

PARECER
Examinado e aprovado pela Secretaria Mun.dos
Negócios Juridicos de acordo com a Lei 8.666/93
Atualizada pela Lei 8.883/94
Bastos-SP, 23 de outubro de 2019
Rafael Teixeira Sebastiani – OAB/SP 355751
Procurador Jurídico

GESTOR DO ÓRGÃO/ENTIDADE:
Nome: MANOEL IRONIDES ROSA
Cargo: PREFEITO MUNICIPAL
CPF: 033.761.228-57 RG: 13.327.411-1
Data de Nascimento: 09/05/1961
Endereço residencial completo: RUA KIYUSUKE SASSAKI, Nº90 BASTOS-SP
E-mail institucional pmbgab@bastos.sp.gov.br
E-mail pessoal:manoel.rosa@live.com
Telefone(s): 014 99721-2285 / 3478-9800
Assinatura:_____

Responsáveis que assinaram o ajuste:

Pelo CONTRATANTE:
Nome: MANOEL IRONIDES ROSA
Cargo: PREFEITO MUNICIPAL
CPF: 033.761.228-57 RG: 13.327.411-1
Data de Nascimento: 09/05/1961
Endereço residencial completo: RUA KIYUSUKE SASSAKI, Nº90 BASTOS-SP
E-mail institucional pmbgab@bastos.sp.gov.br
E-mail pessoal: manoel.rosa@live.com
Telefone(s): 014 99721-2285 / 3478-9800
Assinatura:

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

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

PARECER
Examinado e aprovado pela Secretaria Mun.dos
Negócios Juridicos de acordo com a Lei 8.666/93
Atualizada pela Lei 8.883/94
Bastos-SP, 23 de outubro de 2019
Rafael Teixeira Sebastiani – OAB/SP 355751
Procurador Jurídico

ANEXO LC-03 - DECLARAÇÃO DE DOCUMENTOS À DISPOSIÇÃO DO TCE-SP

CONTRATANTE:PREFEITURA DE MUNICÍPIO DE BASTOS
CNPJ Nº: 45.547.403/0001-93
CONTRATADA:
CNPJ Nº:
CONTRATO N° :.../2019
DATA DA ASSINATURA:
VIGÊNCIA:
OBJETO: CONTRATAÇÃO DE EMPRESA ESPECIALIZADA PARA PRESTAÇÃO DE SERVIÇOS DE TELECOMUNICAÇÕES E TECNOLOGIA DA INFORMAÇÃO, SENDO ELES: (1) PRESTAÇÃO DE SERVIÇO DE TELECOMUNICAÇÕES STFC (SERVIÇO TELEFÔNICO FIXO COMUTADO) NAS MODALIDADES ANALÓGICO E DIGITAL, (2) FORNECIMENTO DE LINK DEDICADO DE ACESSO À INTERNET, (3) FORNECIMENTO E IMPLANTAÇÃO DE SOLUÇÃO DE SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO, NOS TERMOS DAS CONCESSÕES OUTORGADAS PELA AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES – ANATEL.
VALOR (R$):
Declaro(amos), na qualidade de responsável(is) pela entidade supra epigrafada, sob as penas da Lei, que os demais documentos originais, atinentes à correspondente licitação, encontram-se no respectivo processo administrativo arquivado na origem à disposição do Tribunal de Contas do Estado de São Paulo, e serão remetidos quando requisitados.
Em se tratando de obras/serviços de engenharia:
Declaro(amos), na qualidade de responsável(is) pela entidade supra epigrafada, sob as penas da Lei, que os demais documentos originais, atinentes à correspondente licitação, em especial, os a seguir relacionados, encontram-se no respectivo processo administrativo arquivado na origem à disposição do Tribunal de Contas do Estado de São Paulo, e serão remetidos quando requisitados:
a) memorial descritivo dos trabalhos e respectivo cronograma físico-financeiro;
b) orçamento detalhado em planilhas que expressem a composição de todos os seus custos unitários;
c) previsão de recursos orçamentários que assegurem o pagamento das obrigações decorrentes de obras ou serviços a serem executados no exercício financeiro em curso, de acordo com o respectivo cronograma;
d) comprovação no Plano Plurianual de que o produto das obras ou serviços foi contemplado em suas metas;
e) as plantas e projetos de engenharia e arquitetura.

LOCAL e DATA: BASTOS, ... DE ... DE 2019

RESPONSÁVEL: MANOEL IRONIDES ROSA – PREFEITO MUNICIPAL

PARECER
Examinado e aprovado pela Secretaria Mun.dos
Negócios Juridicos de acordo com a Lei 8.666/93
Atualizada pela Lei 8.883/94
Bastos-SP, 23 de outubro de 2019
Rafael Teixeira Sebastiani – OAB/SP 355751
Procurador Jurídico