EDITAL

PREÂMBULO

O Município de Presidente Kennedy, Estado do Espírito Santo, torna público que por intermédio de seu pregoeiro oficial, realizará licitação na modalidade **"PREGÃO ELETRÔNICO" N° 000018/2020**, sob o critério de **"MENOR PRECO POR ITEM",** por meio do site: www.bllcompras.org.br e www.presidentekennedy.es.gov.br para **CONTRATAÇÃO EXCLUSIVA DE MICROEMPRESA OU EMPRESA DE PEQUENO PORTE PARA LICENCIAMENTO DE USO DE SOFTWARE DE SOLUÇÃO DE SEGURANÇA UTM COM DESEMPENHO DE FIREWALL DE 20 GBPS COM SUPORTE, INSTALAÇÃO E TREINAMENTO**, conforme Processo n° 025567/2019, devidamente aprovado pela autoridade competente. O Pregão será realizado por Pregoeiro e Equipe de Apoio, designados pelo Decreto nº 131/2019, de 09 de dezembro de 2019 e regido de acordo com a Lei nº 10.520/2002, Lei Complementar nº 123/2006, Lei nº 8.666/1993 e suas alterações, e pelo Decreto Municipal nº 115/2014, bem como pelas demais normas pertinentes e condições estabelecidas no presente Edital.

1 - DAS INFORMAÇÕES GERAIS

1.1 - **Da retirada do edital -** As microempresas ou empresas de pequeno porte que tiverem interesse em participar do certame deverão retirar o edital no *site* www.presidentekennedy.es.gov.br ou providenciar a cópia que estará à disposição na sala da licitação localizada na Rua Atila Vivacqua, 48 - Centro (em frente ao Banco Banestes), nos dias úteis das 8h às 11h e de 12:30h às 16h, ficando obrigadas a acompanharem as publicações referentes à licitação no Diário Oficial dos Municípios do Espirito Santo - www.diariomunicipal.es.gov.br, tendo em vista a possibilidade de alterações e avisos sobre o procedimento.

1.2 - Do Preço Máximo: O Preço Total Máximo que o Município de Presidente Kennedy-ES se dispõe a pagar é de R$ 34.451,66 (Trinta e quatro mil, quatrocentos e cinquenta e um reais e sessenta e seis centavos), conforme discriminado no **ANEXO II** deste Edital.

1.3 - O Pregão Eletrônico será realizado em sessão pública, por meio da *INTERNET*, mediante condições de segurança - criptografia e autenticação - em todas as suas fases.

1.4 - Os trabalhos serão conduzidos por servidor do órgão promotor do certame, denominado Pregoeiro, mediante a inserção e monitoramento de dados gerados ou transferidos para o aplicativo "pregões" constante da página eletrônica da Bolsa de Licitações e Leilões (BLL).

1.5 - INÍCIO DO ACOLHIMENTO DAS PROPOSTAS: às 16:00h do dia 17/03/2020

1.6 - LIMITE PARA ACOLHIMENTO DAS PROPOSTAS: às 08:00h do dia 31/03/2020

1.7 - DATA E HORÁRIO DE ABERTURA DA SESSÃO PÚBLICA: às 09:00h do dia 31/03/2020

1.8 - PEDIDO DE ESCLARECIMENTOS: Até 03 (três) dias úteis anteriores à data fixada para abertura da sessão pública, exclusivamente por meio eletrônico, via internet, no seguinte endereço eletrônico: pregao@presidentekennedy.es.gov.br.

2 - DO OBJETO

2.1 - O objeto deste Pregão é a **CONTRATAÇÃO EXCLUSIVA DE MICROEMPRESA OU EMPRESA DE PEQUENO PORTE PARA LICENCIAMENTO DE USO DE SOFTWARE DE SOLUÇÃO DE SEGURANÇA UTM COM DESEMPENHO DE FIREWALL DE 20 GBPS COM SUPORTE, INSTALAÇÃO E TREINAMENTO**, em conformidade com quantidades e especificações contidas no Anexo II do presente Edital.

2.3 - **O prazo para entrega** do objeto licitado neste Pregão será **de até 30 (trinta) dias** a contar do recebimento da Ordem de Fornecimento emitida pelo Departamento de Compras.

2.4 - Da Garantia

2.4.1 - Toda solução deverá ser fornecida com suas respectivas licenças de funcionamento em sua capacidade total, com garantia de 03 (três) anos;

2.4.2 - Os equipamentos descritos nas Especificações Técnicas, deverão ter garantia mínima de 36 meses, contados a partir do aceite da fiscalização do contrato;

2.4.3 - Durante o período de garantia, a(s) contratada(s) deverá(ão) disponibilizar um número de contato telefônico da cidade de Vitória (prefixo 027) ou DDG (0800) para abertura de chamado técnico, que deverá ser identificado por um número, por uma data e por uma hora, para que o mesmo possa ser devidamente acompanhado;

2.4.4 - A contratada fornecerá, na data de assinatura do contrato, endereço eletrônico e número de fax para eventual contato que se faça necessário, no caso de indisponibilidade do acesso telefônico;

2.4.5 - A impossibilidade de recebimento da abertura de chamado através de tentativa nos canais de atendimento informados não exime o fornecedor do prazo de manutenção;

2.4.6 - A garantia será prestada na modalidade *on site* e deverá incluir os serviços de manutenção para resolução de problemas de hardware ou software, com substituição de peças ou equipamentos defeituosos, sem qualquer limitação quanto ao quantitativo das mesmas, por outros originais e em estado de novo, compatíveis com as características técnicas especificadas ou superiores, sem quaisquer ônus adicionais para a PMPK;

2.4.7 - Durante o período da garantia do equipamento, a(s) CONTRATADA(s) deverá(ão) prover suporte telefônico para todo problema de hardware, software e configuração dos equipamentos

2.4.8 - O início do atendimento deverá ser realizado em até 24 (vinte e quatro) horas após a abertura do chamado

2.4.9 - As despesas relativas ao transporte de equipamentos, incluindo serviços de manutenção ou substituição, deverão correr por conta da CONTRATADA;

2.4.10 -A fiscalização da PMPK será responsável pelo "ateste" na(s) Nota(s) Fiscal(is), acompanhamento da entregas dos equipamentos e assistência técnica na garantia;

2.4.11 -A(s) CONTRATADA(s) deverá(ão) comunicar por escrito à fiscalização contratual, imediatamente, a impossibilidade de execução de qualquer obrigação contratual, para a adoção das providências cabíveis;

2.4.13 -A falta de peças e/ou equipamentos não poderá ser alegada como motivo de força maior, e não exime a(s) CONTRATADA(s) das penalidades a que está(ão) sujeita(s) pelo não cumprimento dos prazos estabelecidos;

2.4.14 -A(s) CONTRATADA(s) deverá(ão) fornecer correções automáticas das versões de software / firmware durante o período de garantia, caso seja detectado algum problema;

2.4.15 -A(s) CONTRATADA(s) deverá(ão) garantir a total compatibilidade da solução proposta com novas implementações tecnológicas que vierem a ser desenvolvidas pelo fabricante do equipamento fornecido, visando assegurar a evolução e continuidade da base instalada;

2.4.16 -Os empregados da CONTRATADA deverão trajar uniforme com logotipo da empresa e crachá de identificação, enquanto permanecerem nas dependências da CONTRATANTE;

2.4.17 -A(s) CONTRATADA(s) assumirá(ão) inteira responsabilidade pela execução dos eventuais serviço no prazo de garantia, correndo por sua própria conta quaisquer ônus, encargos sociais, trabalhistas, previdenciários, tributos, taxas, licenças e férias, concernentes à contratação, inclusive seguros contra acidentes de trabalho, bem como o de indenizar todo e qualquer dano e prejuízo pessoal ou material que possa advir, direta ou indiretamente, no exercício de suas atividades;

2.4.18 -Os serviços deverão ser executados com observância das especificações técnicas e regulamentação aplicável ao caso, com esmero e correção, refazendo tudo quanto for impugnado pela fiscalização, se necessário;

2.4.20 -As despesas relativas aos eventuais deslocamentos do equipamento ou insumos deverão ocorrer

integralmente por conta da(s) CONTRATADA(s), sem quaisquer ônus adicionais para o CONTRATANTE, durante todo o período de garantia;

2.4.21 -Deverão ser obedecidas as normas de segurança e medicina do trabalho para esse tipo de atividade, ficando por conta da(s) CONTRATADA(s) o fornecimento, antes do início da execução dos serviços, dos Equipamentos de Proteção Individual - EPI, se necessário;

2.4.22 -Indicar, na data de assinatura do contrato, nome e telefone de funcionário que atuará como preposto, conforme preceitua o art. 68 da Lei 8666/93.

2.4.23 -Observações:

2.4.24 -Os prazos deste item poderão ser prorrogados mediante justificativa escrita da(s) CONTRATADA(s), submetida à apreciação do fiscal do CONTRATANTE.

3 - DA DOTAÇÃO ORÇAMENTÁRIA

3.1 - As despesas decorrentes da presente licitação correrão à conta dos seguintes orçamentos: **Secretaria Municipal de Administração**. Projeto/Atividade: **3.107** - Aquisição de Link, implantação e Manutenção da logística digital no município. Elemento de Despesa: 33903900000 - Outros serviços de terceiros - Pessoa Jurídica. Fonte de Recurso: 15300000000 - Transferência da União referente Royalties do Petróleo.

4 - DO REGULAMENTO OPERACIONAL DO CERTAME

4.1 - O certame será conduzido pelo Pregoeiro, que terá, em especial, as seguintes atribuições:

a) coordenar o processo licitatório;

b) receber, examinar e decidir as impugnações e consultas ao edital, apoiado pelo setor responsável pela sua elaboração;

c) conduzir a sessão pública na internet;

d) verificar a conformidade da proposta com os requisitos estabelecidos no instrumento convocatório;

e) dirigir a etapa de lances;

f) verificar e julgar as condições de habilitação;

g) receber, examinar e decidir os recursos, encaminhando à autoridade competente quando mantiver sua decisão;

h) indicar o vencedor do certame;

i) adjudicar o objeto, quando não houver recurso, sendo que, em havendo recursos, competirá ao Secretário da Pasta a adjudicação;

j) conduzir os trabalhos da equipe de apoio;

k) encaminhar o processo devidamente instruído à autoridade superior e propor a homologação.

5 - DAS OBRIGAÇÕES DOS LICITANTES

5.1 - Caberá ao licitante interessado em participar do pregão, na forma eletrônica:

a) Credenciar-se, previamente, junto ao provedor do Sistema, para obtenção da senha de acesso ao sistema eletrônico de compras;
b) Cadastrar o valor da proposta até o prazo estabelecido no item 1.6, exclusivamente por meio eletrônico (via internet).
c) Responsabilizar-se formalmente pelas transações efetuadas em seu nome, assumindo como firmes e verdadeiras suas propostas e lances, inclusive os atos praticados diretamente ou por seu representante, não cabendo ao provedor do sistema ou ao órgão promotor da licitação responsabilidade por eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros;
d) Acompanhar as operações no sistema eletrônico durante o processo licitatório, bem como manter endereço atualizado de correio eletrônico, responsabilizando-se pelo ônus decorrente da perda de negócios diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão;
e) Comunicar imediatamente ao provedor do sistema qualquer acontecimento que possa comprometer o

sigilo ou a inviabilidade do uso da senha, para imediato bloqueio de acesso;

f) Utilizar-se da chave de identificação e da senha de acesso para participar do pregão na forma eletrônica;
g) Solicitar o cancelamento da chave de identificação ou da senha de acesso por interesse próprio.
h) Submeter-se às exigências do Decreto Municipal nº 115/2014, da Lei Federal nº 10.520/02 e, subsidiariamente, da Lei Federal nº 8.666/93, assim como aos termos de participação e condições de contratação constantes neste instrumento convocatório.

6 - CREDENCIAMENTO NO PROVEDOR DO SISTEMA

6.1 - Os licitantes deverão ser previamente credenciados perante o provedor do sistema, para obtenção de acesso ao sistema eletrônico de licitação.

6.2 - O credenciamento dar-se-á pela atribuição de chave de identificação e de senha, pessoal e intransferível, para acesso ao sistema eletrônico.

6.3 - A chave de identificação e a senha poderão ser utilizadas em qualquer pregão eletrônico, salvo quando canceladas por solicitação do credenciado ou em virtude de sua inabilitação perante o cadastro de fornecedores.

6.4 - A perda da senha ou a quebra de sigilo deverão ser comunicadas imediatamente ao provedor do sistema, para imediato bloqueio de acesso.

6.5 - O uso da senha de acesso pelo licitante é de sua responsabilidade exclusiva, incluindo qualquer transação efetuada diretamente ou por seu representante, não cabendo ao provedor do sistema ou ao órgão promotor da licitação, responsabilidade por eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros.

6.6 - O credenciamento junto ao provedor do sistema implica a responsabilidade legal do licitante ou de seu representante legal e a presunção de sua capacidade técnica para realização das transações inerentes ao pregão eletrônico.

7 - DAS CONDIÇÕES GERAIS PARA A PARTICIPAÇÃO

7.1 - Poderão participar desta licitação somente microempresas ou empresas de pequeno porte do ramo de atividade pertinente ao objeto licitado, que atenderem a todas as exigências deste edital e seus anexos, além das disposições legais, independentemente de transcrição.

7.2 - Todos os **DOCUMENTOS DE HABILITAÇÃO** - **deverão** ser apresentados em original, por qualquer processo de cópia autenticada por tabelião de nota ou por servidor do setor de licitações desta Prefeitura, sendo passíveis de consulta quanto à veracidade, a critério exclusivo do Pregoeiro/Equipe de Apoio.

7.2.1 - Serão aceitas somente cópias legíveis, não sendo aceitos documentos cujas data estejam rasuradas.

7.3 - O Município de Presidente Kennedy reserva-se o direito de solicitar o original de qualquer documento, sempre que julgar necessário.

7.4 - Poderão participar deste Pregão somente pessoas jurídicas **que desenvolvam as atividades objeto desta licitação** e que atendam às exigências deste edital.

7.5 - Não é admitida a participação nesta licitação de empresas que estejam cumprindo pena de suspensão

temporária de participação em licitação e/ou impedimento de contratar com a Administração; que tenham sido declaradas inidôneas para licitar ou contratar com qualquer órgão público; ou que se subsumem às disposições dos artigos 9º e inciso V, do art. 27, da Lei nº 8.666/93.

7.6 - Estarão impedidos de participar de qualquer fase do processo, interessados que se enquadrarem em uma ou mais das situações a seguir:
a) estejam constituídos sob a forma de consórcio;
b) estejam cumprindo as penalidades previstas no art. 87, inciso III da Lei Federal n° 8.666/93 e no art. 7° da Lei Federal n° 10.520/02, desde que impostas pela própria Administração Pública Municipal;
c) estejam cumprindo a pena prevista no art. 87, inciso IV da Lei Federal n° 8.666/93, ainda que imposta por ente federativo diverso do estado do Espírito Santo;
d) não cumpram o disposto no art. 9° da Lei n° 8.666/93 e alterações.

8 - DO RECEBIMENTO E ABERTURA DAS PROPOSTAS E DATA DO PREGÃO

8.1 - O fornecedor deverá observar as datas e os horários limites previstos para a abertura da proposta, atentando também para a data e horário do início da disputa.

9 - DA REFERÊNCIA DE TEMPO

9.1 - Todas as referências de tempo no Edital, no Aviso e durante a Sessão Pública observarão, obrigatoriamente, o horário de Brasília - DF e, dessa forma, serão registradas no sistema eletrônico e na documentação relativa ao certame.

10 - DA SESSÃO DE ABERTURA E JULGAMENTO DAS PROPOSTAS

10.1 - Os licitantes deverão cadastrar a proposta com a descrição do objeto ofertado e com o preço, exclusivamente por meio do sistema eletrônico, observando a data e o horário limite para o seu acolhimento, quando, então, encerrar-se-á, automaticamente, a fase de recebimento de propostas.

10.1.1 - Ao realizar o cadastro dos valores nos respectivos itens, a licitante fica ciente e anui com os seguintes termos:

a) A validade da proposta não será inferior a 90 (noventa) dias, contados da data de abertura da mesma.

b) Declara, sob as penas da lei, principalmente a disposta no art. 7º da Lei nº 10.520/2002, que satisfaz plenamente todas as exigências habilitatórias previstas no certame epigrafado, em obediência ao disposto no art. 4º, VII da Lei nº 10.520/2002.

10.1.2 - Deverá ser cadastrado no sistema o preço **UNITÁRIO** ofertado por Item.

10.1.3 - Deverá ser cadastrado no sistema a MARCA do produto.

10.2 - A participação no pregão eletrônico dar-se-á pela utilização da senha privativa do licitante.

10.3 - Para participação no pregão eletrônico, o licitante deverá manifestar, em campo próprio do sistema eletrônico, que cumpre plenamente os requisitos de habilitação e que sua proposta está em conformidade com as exigências do instrumento convocatório.

10.4 - A declaração falsa relativa ao cumprimento dos requisitos de habilitação e proposta sujeitará o licitante às sanções previstas na legislação de regência, sem prejuízo de qualquer sanção criminal cabível.

10.5 - Até a abertura da sessão, os licitantes poderão alterar a proposta anteriormente cadastrada.

10.5.1 - Após abertura do certame, não cabe desistência da proposta, salvo por motivo justo decorrente de fato superveniente e aceito pelo pregoeiro.

10.5.2 - A(s) empresa(s) vencedora(s) deverão estar cientes de que NÃO serão aceitas propostas comerciais atualizadas com preços unitários divergentes dos preços praticados no mercado. Se necessário, será procedida análise para verificação de discrepâncias.

10.5.3 - A proposta será desclassificada se for contrária, expressamente, às normas e exigências deste edital.

10.5.4 - As propostas, sempre que possível, deverão trazer as mesmas expressões contidas no Anexo II, evitando sinônimos técnicos, omissões ou acréscimos referentes à especificação do objeto.

10.5.5 - Não serão aceitas propostas parciais (quantidade inferior), com relação a cada item.

11 - DO JULGAMENTO E CLASSIFICAÇÃO DAS PROPOSTAS

11.1 - Esta licitação será julgada sob o critério de MENOR PREÇO POR ITEM.

11.2 - Aberta a sessão pública, o pregoeiro verificará as propostas apresentadas, desclassificando aquelas que não estejam em conformidade com os requisitos estabelecidos no edital.

11.3 - A desclassificação de proposta será fundamentada e registrada no sistema, com acompanhamento em tempo real por todos os participantes.

11.4 - As propostas contendo a descrição do objeto, valor e eventuais anexos estarão disponíveis na internet.

11.5 - O sistema disponibilizará campo próprio para troca de mensagens entre o pregoeiro e os licitantes.

11.6 - O sistema ordenará, automaticamente, as propostas classificadas pelo pregoeiro, sendo que somente estas participarão da fase de lance.

11.7 - Classificadas as propostas, considerando-se o critério de MENOR PREÇO POR ITEM, o pregoeiro dará início à fase competitiva, quando então os licitantes poderão encaminhar lances exclusivamente por meio do sistema eletrônico.

11.8 - No que se refere aos lances, o licitante será imediatamente informado do seu recebimento e do valor consignado no registro.

11.9 - Os licitantes poderão oferecer lances sucessivos, observados o horário fixado para abertura da sessão e as regras estabelecidas neste edital.

11.10 - O licitante somente poderá oferecer lance inferior ao último por ele ofertado e registrado pelo sistema.

11.11 - Não serão aceitos dois ou mais lances iguais, prevalecendo aquele que for recebido e registrado primeiro.

11.12 - Durante a sessão pública, os licitantes serão informados, em tempo real, do valor do menor lance registrado, vedada a identificação do licitante.

11.13 - A fase competitiva da sessão pública será encerrada por decisão do pregoeiro, dando-se início ao tempo aleatório do sistema.

11.14 - No decurso do tempo aleatório concedido pelo sistema para oferecimento de lances, o sistema eletrônico encerrará, aleatoriamente, dentro de um período de até 30 (trinta) minutos, a recepção de lances, após encerramento do tempo normal pelo pregoeiro.

11.15 - Após o encerramento da etapa de lances da sessão pública, o pregoeiro poderá encaminhar, pelo sistema eletrônico, contraproposta ao licitante que tenha apresentado lance mais vantajoso, para que seja obtida melhor proposta, observado o critério de julgamento, não se admitindo negociar condições diferentes daquelas previstas no edital.

11.15.1 - Na hipótese de comparecer apenas 01 (um) licitante na sala de disputa, passar-se-á, automaticamente, à fase de contraproposta, prevista no item 11.15.

11.16 - A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais licitantes.

11.17 - No caso de desconexão do pregoeiro, no decorrer da etapa de lances, se o sistema eletrônico permanecer acessível aos licitantes, os lances continuarão sendo recebidos, sem prejuízo dos atos realizados.

11.18 - Se a desconexão do pregoeiro persistir por tempo superior a dez minutos, a sessão do pregão na forma eletrônica será suspensa e reiniciada somente após comunicação aos participantes, no endereço eletrônico utilizado para divulgação.

12 - DA HABILITAÇÃO DO LICITANTE VENCEDOR

12.1 - Encerrada a etapa de lances e o exame da proposta classificada em primeiro lugar quanto à compatibilidade do preço em relação ao estimado para contratação, exequibilidade e adequação, o pregoeiro verificará a habilitação do licitante arrematante conforme disposições deste Edital.

12.2 - Constatado o atendimento quanto à compatibilidade do preço, em relação ao estimado para contratação, e quanto às exigências do edital, o licitante que ofertou o menor preço será declarado vencedor e será solicitada a apresentação dos documentos de habilitação.

12.3 - A licitante **deverá** apresentar, em 05 (cinco) dias úteis, a partir da solicitação do pregoeiro, quando da declaração do vencedor, todos os documentos e anexos exigidos para habilitação.

12.3.1 - ***As empresas detentoras da melhor proposta que, ao serem convocadas para apresentarem suas documentações no prazo supracitado, isto é, em cinco dias úteis, não o fizerem, sofrerão as sanções administrativas previstas nos termos definidos no art. 9º da Instrução Normativa SCL nº 08/2017, aprovada pelo Decreto nº 041/2019.***

12.4 - Os documentos e anexos exigidos para fins de habilitação, **deverão** ser protocolizados em original ou por cópia autenticada, no Setor de Protocolo desta Prefeitura localizado na Rua Lucio Moreira Filho, Sn - Centro (ao lado da Biblioteca Pública Municipal), em dias úteis, no horário de 08h as 11h e 12:30h às 17h,

exceto a sexta-feira que será de 08h às 11h e 12:30h às 16h, no prazo de 05 (cinco) dias úteis, a contar do encerramento da sessão de disputa e solicitação do pregoeiro.

12.5 - Para fins de habilitação, a verificação pelo órgão promotor do certame nos sítios oficiais de órgãos e entidades emissoras de certidões constitui meio legal de prova.

12.6 - Se a proposta não for aceitável, ou se o licitante não atender às exigências habilitatórias, ou se recusar-se a assinar o contrato, o pregoeiro examinará a oferta subsequente e a respectiva documentação de habilitação, na ordem de classificação, e assim sucessivamente, até a apuração de uma que atenda às exigências do edital.

12.7 - Nas hipóteses previstas no item anterior, o pregoeiro poderá negociar diretamente com o proponente para que seja obtido melhor preço, tendo sempre como parâmetro a menor oferta apresentada no certame.

12.8 - Quando verificada discrepância relevante entre o preço da menor oferta obtida no certame e aquele decorrente da negociação com o licitante remanescente, será facultado à Administração revogar o procedimento licitatório, mediante despacho fundamentado, assegurada a ampla defesa e o contraditório.

12.9 - Documento de Habilitação

12.9.1 - Habilitação Jurídica

a) Ato Constitutivo, Estatuto ou Contrato Social em vigor, devidamente registrado, em se tratando de sociedade comercial, no caso de sociedade por ações, acompanhado de documentos de eleição dos seus administradores, ou Registro Comercial no caso de empresa individual;
b) Decreto de autorização, em se tratando de empresa ou sociedade estrangeira em funcionamento no País, e ato de registro ou autorização para funcionamento expedido pelo órgão competente, quando a atividade assim o exigir;
c) Inscrição do ato constitutivo, no caso de sociedade civil, acompanhada de prova de diretoria em exercício;

12.9.2 - Regularidade Fiscal e Trabalhista

a) Prova de Inscrição no Cadastro Nacional de Pessoa Jurídica - Cartão CNPJ regular;
b) Prova de regularidade com a Fazenda Federal ou Certidão Conjunta prevista na Portaria MF nº 358, de 05 de setembro de 2014;
c) Prova de regularidade com a Seguridade Social - INSS ou Certidão Conjunta prevista na Portaria MF nº 358, de 05 de setembro de 2014;
d) Prova de regularidade com o FGTS (Fundo de Garantia do Tempo de Serviço);
e) Prova de regularidade com a Fazenda Estadual da sede da empresa;
f) Prova de regularidade com a Fazenda Municipal da sede da empresa;
g) Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei n° 5.452, de 1o de maio de 1943, em atendimento a Lei 12.440/11;

12.9.3 - Qualificação Técnica

a) Comprovação de aptidão para o fornecimento do(s) objeto(s) licitado(s), mediante apresentação de declaração em papel timbrado, firmada por pessoas jurídicas públicas e/ou privadas, que sendo clientes da licitante, atestem a capacidade da mesma para proceder o fornecimento do(s) objeto(s) licitado(s); **(com identificação e endereço da pessoa jurídica emitente, nome e cargo do signatário).**

12.9.4 - Qualificação Econômica - financeira

a) Apresentação de Certidão Negativa de Falência ou Certidão de Recuperação Judicial, emitida pelo(s)

Cartório(s) Distribuidor(es) da sede ou domicílio da empresa licitante, emitida no máximo 90 (noventa) dias, quando outro prazo de validade não estiver expresso no documento.

12.9.5- Declaração

a) Declaração Conjunta, em papel timbrado da empresa, conforme **ANEXO III** deste Edital.

12.9.6 - Proposta Atualizada

a) A licitante **DEVERÁ** apresentar **PROPOSTA DE PREÇOS ATUALIZADA**, contendo a descrição do objeto, os valores e assinatura do representante da empresa.

12.9.6 - Da Comprovação da Condição de MICROEMPRESA OU EMPRESA DE PEQUENO PORTE

12.9.6.1 - Os licitantes que invocarem a condição de microempresa ou empresa de pequeno porte, na proposta comercial feita no sistema provedor **no período de acolhimento de propostas**, para fins de exercício de quaisquer benefícios previsto na Lei Complementar nº 123/2006 e suas alterações, em especial a Lei Complementar nº 147/2014, deverão apresentar além da documentação prevista no item 12.9, na fase de habilitação, os seguintes documentos:

a) Apresentar a CERTIDÃO EXPEDIDA PELA JUNTA COMERCIAL, seguindo o delineamento do art. 8º da Instrução Normativa nº 103/2007 do Departamento Nacional de Registro do Comércio, **OU** caso a licitante enquadrada como microempresa (ME) ou empresas de pequeno porte (EPP) seja optante pelo Sistema Simples Nacional de Tributação, regido pela lei Complementar nº 123/2006, deverá apresentar o comprovante de opção obtido no site do Ministério da Fazenda (<http://www8.receita.fazenda.gov.br/SimplesNacional>).

a.1) Caso o Licitante opte por apresentar a certidão expedida pela Junta Comercial ou pelo Cartório de Registro, esta deverá atestar **expressamente** o enquadramento da empresa como ME ou EPP, sob pena de perda do direito de usufruir dos benefícios da LC nº 123/2006.

a.2) A empresa que apresentar a Certidão expedida pela Junta Comercial ou pelo Cartório de Registro exigida na alínea 'a" deverá apresentar com data de expedição a partir de 01 de janeiro de 2015, ou data posterior, em caso de qualquer alteração do contrato social.

12.10 - As certidões exigidas no item 12.9.2 deverão conter o mesmo CNPJ apresentado pelo licitante no momento do credenciamento.

12.11 - Figuram como exceções as certidões cuja abrangência atinge tanto a empresa Matriz, quanto as Filiais (INSS e PGFN/Receita Federal).

12.12 - Aplicar-se-ão às microempresas e aos microempreendedores individuais que se enquadram nas disposições contidas na Lei Complementar nº 123/2006, de 14 de dezembro de 2006 (Estatuto da Microempresa e da Empresa de Pequeno Porte) as prescrições referentes à regularidade fiscal (artigos 42 e 43).

12.13 - O Pregoeiro, durante a análise do envelope de HABILITAÇÃO, procederá à validação nos sítios dos órgãos oficiais (Receita Federal, PGFN, Caixa Econômica Federal, Previdência Social, Secretarias da Fazenda) expedidoras das certidões apresentadas.

13 - DOS RECURSOS, IMPUGNAÇÕES E PEDIDOS DE ESCLARECIMENTO

13.1 - Dos atos relacionados a este procedimento licitatório cabem os recursos previstos na Lei nº 10.520/02 e na Lei 8.666/93 e suas alterações, sendo a autoridade superior para o recurso o Secretário Municipal.

13.1.1 - Declarada a licitante habilitada, qualquer licitante poderá, durante a sessão pública, de forma imediata e motivada, em campo próprio do sistema, manifestar sua intenção de recorrer, quando lhe será concedido o prazo de 03 (três) dias para apresentação das razões de recurso, ficando as demais licitantes desde logo intimadas para, querendo, apresentarem contrarrazões em igual prazo, que começará a contar do término do prazo do recorrente, sendo-lhes assegurada vista imediata dos autos.

13.1.2 - A falta de manifestação imediata e motivada da empresa licitante importará na decadência do direito de recurso, ficando o pregoeiro autorizado a adjudicar o objeto ao licitante declarado vencedor.

13.1.3 - Para efeito no disposto acima, manifestação imediata é aquela efetuada via eletrônica - internet -, no período máximo de 30 (trinta) minutos após o pregoeiro comunicar aos participantes, por meio do sistema eletrônico, o resultado da classificação final; e manifestação motivada é a descrição sucinta e clara do fato que motivou a licitante a recorrer.

13.1.4 - O acolhimento de recurso importará na invalidação apenas dos atos insuscetíveis de aproveitamento.

13.1.5 - As razões e contrarrazões de recurso deverão ser dirigidos ao Pregoeiro e protocolizados no Setor de Protocolo desta Prefeitura localizada na Rua Lucio Moreira Filho, Sn - Centro (ao lado da Biblioteca Pública Municipal), em dias úteis, no horário de 08h às 11h e 12:30h às 17h, exceto a sexta-feira que será de 08h às 11h e 12:30h às 16h, OU encaminhadas pelo e-mail pregao@presidentekennedy.es.gov.br OU ainda em campo próprio do sistema da BLL.

13.1.6 - Os recursos obedecerão aos seguintes critérios:
a) serão observadas as condições da lei 10.520/02 e, no que couber, as condições do artigo 109 da Lei 8.666/93;
b) serem dirigidos ao(a) Pregoeiro(a), devidamente fundamentados e, quando for o caso, acompanhados de documentação pertinente;
c) serem assinados por representante legal do licitante ou Procurador com poderes específicos, hipótese em que deverá ser anexado o instrumento procuratório (se ausente nos autos);
d) não serão aceitos recursos via fax ou e-mail.

13.2 - As impugnações deverão observar os seguintes critérios:

13.2.1 - A impugnação do edital deverá ser promovida através de protocolo na sede da Prefeitura Municipal de Presidente Kennedy, seguindo as condições e os prazos previstos no art. 41 da Lei nº 8.666/1993. As impugnações deverão ser dirigidas ao Pregoeiro e protocolizadas no Setor de Protocolo desta Prefeitura localizada na Rua Lucio Moreira Filho, Sn - Centro (ao lado da Biblioteca Pública Municipal), em dias úteis, no horário de 08h às 11h e 12:30h às 17h, exceto a sexta-feira que será de 08h às 11h e 12:30h às 16h, OU encaminhadas pelo e-mail pregao@presidentekennedy.es.gov.br OU ainda em campo próprio do sistema da BLL.

13.2.2 - A impugnação do edital deverá ser dirigida ao Pregoeiro, indicando os números do Pregão e do Processo Administrativo. No mesmo momento deverá ser juntado documento que comprove a aptidão do signatário para a representação da empresa licitante.

13.2.3 - O Município de Presidente Kennedy julgará e decidirá sobre a impugnação no prazo de até 03 (três) dias úteis.

13.2.4 - No caso de acolhimento da impugnação, será designada nova data para a realização do certame, exceto quando, inquestionavelmente, a alteração não afetar a formulação das propostas.

13.3 - Os pedidos de esclarecimentos referentes a este processo licitatório deverão ser enviados ao pregoeiro, até três dias úteis anteriores à data fixada para abertura da sessão pública, exclusivamente por meio eletrônico, via internet, no seguinte endereço eletrônico: pregao@presidentekennedy.es.gov.br.

14 - DA HOMOLOGAÇÃO E DA ADJUDICAÇÃO

14.1 - Caso não haja interesse recursal manifestado na sessão o Pregoeiro é quem adjudicará o objeto, sendo que esta adjudicação não produzirá efeitos até a homologação pela autoridade superior.

14.2 - A classificação das propostas, o julgamento da proposta e da habilitação serão submetidos à autoridade superior para deliberação quanto a sua homologação e a adjudicação do objeto da licitação, caso ocorra recurso.

14.3 - Decididos os recursos e constatada a regularidade dos atos praticados, a autoridade competente adjudicará o objeto e homologará o procedimento licitatório.

15 - DA ASSINATURA DO CONTRATO

15.1 - Após a homologação, a empresa vencedora será convocada para assinar o contrato no prazo de até 05 (cinco) dias úteis.

15.2 - A Administração poderá prorrogar o prazo fixado no item acima, por igual período, nos termos do art. 64, §1° da Lei Federal n° 8.666/93, quando solicitado pelo licitante vencedor, durante o seu transcurso, e desde que ocorra motivo justificado, aceito pela Administração.

15.3 - É facultado a Administração, quando a convocada não comparecer no prazo estipulado no subitem 15.1, não apresentar situação regular no ato da assinatura do contrato ou, ainda, recusar-se a assiná-lo, injustificadamente, convocar as LICITANTES remanescentes, na ordem de classificação, sem prejuízo da aplicação das sanções cabíveis, observando o disposto no item 18.

15.4 - A contratada fica obrigada a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões de até 25% (vinte e cinco por cento) do valor inicial atualizado do contrato, conforme o Art. 65, § 1º da Lei nº 8.666/93.

15.5 - PARA FINS DE ASSINATURA DO CONTRATO

a) **A LICITANTE deverá apresentar** declaração do Fabricante informando que a LICITANTE está autorizada a comercializar, instalar, configurar e prestar suporte técnico na solução ofertada;

b) **A LICITANTE deverá apresentar** declaração do Fabricante informando que seu produto atende a todas as características e funcionalidades exigidas e contidas neste edital, devidamente acompanhada da indicação do (s) Código (s) e Nome (s) dos seus Softwares propostos para fornecimento do objeto deste edital;

c) **A LICITANTE deverá apresentar** declaração que possuir técnicos certificados pelo Fabricante da solução para comprovar qualificação para execução do serviço.

d) A LICITANTE deverá emitir declaração que cumpre todos os requisitos técnicos do edital se responsabilizando por isso, sendo que os requisitos técnicos serão validados pela equipe técnica de homologação.

16 - DA RETIRADA DA ORDEM DE FORNECIMENTO

16.1 - O Município de Presidente Kennedy convocará a(s) licitante(s) para retirar(em) a(s) respectiva(s)

Ordem(ns) de **Fornecimento** relativa ao presente pregão.

16.2 - O prazo para a retirada da Ordem de **Fornecimento** após a convocação é de 5 (cinco) dias úteis.

16.3 - No caso de a (s) licitante (s) vencedora (s) do certame, dentro do prazo de validade da (s) sua respectiva proposta, não atender (em) à exigência do item anterior (16.2), desatender o disposto no Termo de Referência (Anexo I); demais condições; não assinar o contrato ou deixar fornecer o produto e a sua instalação, objeto desta licitação, aplicar-se-á o previsto no inc. XVI, do art. 4º, da Lei nº 10.520/02.

17 - DO PAGAMENTO

17.1 - O(s) pagamento(s) será(ão) efetuado(s) mediante a apresentação de documento fiscal hábil, sem emendas ou rasuras, relativo ao(s) fornecimento **efetivamente** entregue, que deverá ser encaminhada em nome do Município de Presidente Kennedy, com fornecimento dos materiais discriminados, a qual, após a atestação do setor competente, será encaminhada para processamento do pagamento, e realizada a aceitação dos mesmos, ocorrendo o pagamento em até 30 (trinta) dias, após o recebimento da nota fiscal.

17.1.1 - O documento fiscal hábil (Nota Fiscal ou equivalente) deverá conter o mesmo CNPJ do Contrato Social, Ato Constitutivo ou Estatuto apresentado no ato do credenciamento.

17.1.2 - Os pagamentos somente serão efetuados após a execução dos serviços, conforme as exigências dos ANEXOS I e II e apresentação do relatório dos serviços prestados.

17.1.3 - Ocorrendo erros na apresentação do(s) documento(s) fiscal(is), o(s) mesmo(s) será(ão) devolvido(s) à contratada para correção, ficando estabelecido que o prazo para pagamento será contado a partir da data de apresentação da nova fatura, devidamente corrigida.

17.2 - O Município de Presidente Kennedy poderá deduzir do pagamento importâncias que a qualquer título lhe forem devidos pela contratada, em decorrência de inadimplemento contratual.

17.3 - O pagamento das faturas somente será feito em carteira ou cobrança simples, sendo expressamente vedada à contratada a cobrança ou desconto de duplicatas por meio da rede bancária ou de terceiros.

17.4 - Para a efetivação do pagamento o licitante deverá manter as mesmas condições previstas neste edital no que concerne à PROPOSTA e à HABILITAÇÃO.

17.5 - O PAGAMENTO SOMENTE SERÁ EFETUADO nos termos definidos pela Instrução Normativa SFI n° 001/2013 aprovada pelo Decreto Municipal n° 087/2015 e MEDIANTE APRESENTAÇÃO DAS CERTIDÕES ABAIXO RELACIONADAS**, JUNTAMENTE COM AS NOTAS FISCAIS:**

a) Prova de regularidade com a Fazenda Federal; Prova de regularidade (certidão) com a Seguridade Social - INSS; Prova de regularidade (certidão) com o FGTS (Fundo de Garantia do Tempo de Serviço); Prova de regularidade com a Fazenda Estadual sede da licitante; Prova de regularidade com a Fazenda do Município sede da licitante; Prova de regularidade com a Fazenda do Município de Presidente Kennedy e Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei n° 5.452, de 1° de maio de 1943, em atendimento a Lei 12.440/11, através de certidões expedidas pelos órgãos competentes, que estejam dentro do prazo de validade expresso na própria certidão.

b) A cada solicitação de pagamento a Contratada deverá comprovar que mantém todas as condições de

habilitação e qualificações exigidas, juntando à solicitação de pagamento toda documentação apresentada no momento da licitação.

17.6 - O MUNICÍPIO EFETUARÁ TODOS OS PAGAMENTOS POR SISTEMA DE ORDEM BANCÁRIA, NÃO SENDO REALIZADAS EMISSÃO DE CHEQUES, portanto, as empresas deverão informar os dados bancários para recebimento dos pagamentos.

18 - PENALIDADES E SANÇÕES

18.1 - A empresa contratada deverá observar rigorosamente as condições estabelecidas para prestação dos serviços adjudicados, sujeitando-se às penalidades constantes no artigo 86 e 87 da Lei 8.666/93 e suas alterações e do art. 7º da Lei 10.520/02, a saber:

18.1.1 - Suspensão do direito de licitar pelo período de até 02 (dois) anos, em caso de manter-se inerte por período superior a 15 (quinze) dias do ato que deva praticar;

18.1.2 - Multa pelo atraso em prazo estipulado após a adjudicação do objeto, calculada pela fórmula:

M = 0,5 x C x D
onde:
M = valor da multa
C = valor da obrigação
D = número de dias em atraso

18.1.3 - Pelo não fornecimento e prestação dos serviços contratados, multa de 2 % (dois por cento) do valor do Contrato, e nessa hipótese, poderá ser revogada a licitação ou convocar os licitantes remanescentes, na ordem de classificação, para fazer o fornecimento e prestação de serviços, nas mesmas condições propostas pelo primeiro classificado;

18.1.4 - Declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos da punição, ou até que seja promovida a reabilitação perante a autoridade que aplicou a penalidade, o que será concedido sempre que a CONTRATADA ressarcir o Município pelos prejuízos resultantes e depois de decorrido o prazo da sanção aplicada;

18.1.4.1 - A sanção de "declaração de inidoneidade" é de competência do Secretário da Pasta, facultada a defesa do interessado no respectivo processo, no prazo de 10 (dez) dias da abertura de vista ao processo, podendo a reabilitação ser requerida após 02 (dois) anos de sua aplicação.

18.2 - Juntamente com a aplicação das penalidades e sanções prevista nos itens acima, deverá ser observado pela Administração o disposto na INSTRUÇÃO NORMATIVA DO SISTEMA DE COMPRAS LICITAÇÕES E CONTRATOS - SCL Nº 007/2016, aprovada pelo Decreto Municipal Nº 58/2016.

19 - DISPOSIÇÕES FINAIS

19. 1 - O proponente é responsável pela fidelidade e legitimidade das informações prestadas e dos documentos apresentados em qualquer fase da licitação. A falsidade de qualquer documento apresentado ou a inverdade das informações nele contidas implicará a imediata desclassificação do proponente que o tiver apresentado, ou, caso tenha sido o vencedor, a rescisão do ajuste ou pedido de compra, sem prejuízo das demais sanções cabíveis.

19.2 - Ao apresentar a proposta, o licitante assume que está fazendo isso de forma absolutamente independente e que, acaso se apresente, em qualquer momento, a formação de cartel ou qualquer conluio, a Administração adotará os meios necessários para as devidas averiguações e as respectivas sanções.

19.3 - É facultado ao Pregoeiro, ou à autoridade a ele superior, em qualquer fase da licitação, promover diligências com vistas a esclarecer ou a complementar a instrução do processo, vedada a criação de exigência não prevista neste edital.

19.4 - Os licitantes intimados para prestar quaisquer esclarecimentos adicionais deverão fazê-lo no prazo determinado pelo Pregoeiro, sob pena de desclassificação.

19.5 - Em caso de dúvida quanto à autenticidade de assinatura constante em documento apresentado por licitante, poder-se-á diligenciar no intuito de saná-la, inclusive concedendo prazo para o reconhecimento de firma.

19.6 - Em caso de dúvida quanto à autenticidade do atestado de capacidade técnica apresentado pelo licitante, poder-se-á diligenciar no intuito de saná-la, inclusive com concessão de prazo para apresentar a nota fiscal que originou o atestado.

19.7 - O desatendimento de exigências formais não essenciais não importará no afastamento do proponente, desde que seja possível a aferição da sua qualificação e a exata compreensão da sua proposta.

19.8 - As normas que disciplinam este Pregão serão sempre interpretadas em favor da ampliação da disputa entre os proponentes, desde que não comprometam o interesse da Administração, o princípio da isonomia, a finalidade e a segurança da contratação.

19.9 - As decisões referentes a este processo licitatório poderão ser comunicadas aos proponentes por qualquer meio de comunicação que comprove o recebimento ou, ainda, mediante publicação no Diário Oficial dos Municípios do Espirito Santo.

19.10 - Este Edital será regido pelas regras e pelos princípios publicistas, pela Lei nº 10.520/02, pela Lei nº 8.666/93 com suas alterações, e pela Lei Complementar nº 123/06, independente da transcrição das normas vigentes e os casos não previstos serão decididos pelo Pregoeiro com base no ordenamento jurídico vigente.

19.11 - A participação do licitante nesta licitação implica aceitação de todos os termos deste Edital.

19.12 - A autoridade competente para aprovação do procedimento licitatório somente poderá revogá-lo em face de razões de interesse público, por motivo de fato superveniente devidamente comprovado, pertinente e suficiente para justificar tal conduta, devendo anulá-lo por ilegalidade, de ofício ou por provocação de qualquer pessoa, mediante ato escrito e fundamentado.

19.13 - Os licitantes não terão direito à indenização em decorrência da anulação do procedimento licitatório, ressalvado o direito da contratada de boa-fé de ser ressarcido pelos encargos que tiver suportado no cumprimento do ajuste.

19.14 - A nulidade do procedimento licitatório induz a do contrato, ressalvando o disposto no parágrafo único do art. 59, da Lei nº 8.666/93.

19.15 - No caso de desfazimento do processo licitatório, fica assegurada a ampla defesa e o contraditório.

19.16 - É parte integrante deste Edital:

Anexo I - Termo de Referência;
Anexo II - Descritivo, Quantitativo e Valores Médios dos Objetos/Serviço.
Anexo III - Modelo de Declaração Conjunta;
Anexo IV - Minuta de Contrato;

Presidente Kennedy-ES, 06 de fevereiro de 2020.

Leonardo dos Santos
Pregoeiro Oficial

EDITAL

ANEXO I - TERMO DE REFERÊNCIA

OBJETO

1.1. Aquisição de Licença de software de segurança da informação do tipo UTM (Unified Threat Management) com os seguintes recursos: Filtro de pacotes com controle de estado, soluções do tipo (QoS, Balanceamento de serviços, Redundância de links, VPN IPSec, DHCP e DNS) e de licenciamento por subscrição: Filtro de conteúdo web, Interceptação SSL, Filtro de aplicações, Controle da web 2.0, Inspeção com proteção contra-ataques de Malwares, vírus, worm, e aplicativos maliciosos, Intrusion protect system, Advanced threat protection e Antimalware http/s.

JUSTIFICATIVA TÉCNICA

1.2. A Interligação de todos os prédios públicos da Administração Municipal de Presidente Kennedy em uma única rede, tem como objetivo efetuar a convergência no acesso as informações públicas e o acesso à Internet de forma segura e centralizada.

1.3. São necessários tecnologias de Segurança da Informação, destinadas a proteção do tráfego de dados, que ocorre entre as redes locais de cada Órgão da Administração Municipal, bem como as informações com origem ou destino à Internet e a segregação de segmentos de rede.

1.4. São necessários Controles de Acesso e Monitoramento Avançado do tráfego de dados que ocorre nas Instituições de Ensino Municipais visando segregar a Rede Administrativa (Secretaria, Coordenação e Pedagógica), Rede dos Laboratórios de Informática, Acesso a Sistemas Internos e Acessos vindo de Acessos Externos (Internet), bem como redes de acesso público, como futura rede Wifi Visitantes.

HABILITAÇÃO

1.5. Atestado de Capacidade Técnica, em nome da LICITANTE, expedido por pessoa jurídica de direito público ou privado, que comprove o fornecimento de software similares aos ofertados, serviços de instalação, configuração e suporte técnico;

PARA FINS DE ASSINATURA DO CONTRATO

1.6. **A LICITANTE deverá apresentar** declaração do Fabricante informando que a LICITANTE está autorizada a comercializar, instalar, configurar e prestar suporte técnico na solução ofertada;

1.7. **A LICITANTE deverá apresentar** declaração do Fabricante informando que seu produto atende a todas as características e funcionalidades exigidas e contidas neste edital, devidamente acompanhada da indicação do (s) Código (s) e Nome (s) dos seus Softwares propostos para fornecimento do objeto deste edital;

1.8. **A LICITANTE deverá apresentar** declaração que possuir técnicos certificados pelo Fabricante da solução para comprovar qualificação para execução do serviço.

1.9. A LICITANTE deverá emitir declaração que cumpre todos os requisitos técnicos do edital se responsabilizando por isso, sendo que os requisitos técnicos serão validados pela equipe técnica de homologação.

DOS REQUISITOS COMUNS PARA TODOS OS ITENS

1.10. Os produtos que compõe a Solução de Segurança devem todos ser produzidos pelo mesmo fabricante;

1.11. O software deve ser instalado em máquina virtual ou opcionalmente, e com a devida solicitação, em appliance fornecido definitivamente pela LICITANTE VENCEDORA sem custos adicionais para a CONTRATANTE. A LICITANTE deve informar na proposta comercial e na tabela de formação de preços a marca do(s) produto(s) ofertado(s);

1.12. Para os itens do objeto deverão ser fornecidos todos os itens de hardware ou acessórios para o perfeito funcionamento do software, incluindo licenças, conectores, interfaces, suportes, braços organizadores de cabos e demais equipamentos necessários para instalação e funcionamento da solução, em plena compatibilidade com as especificações constantes neste documento e recomendadas pelo fabricante

1.13. A LICITANTE deverá realizar a instalação dos produtos de segurança contratados pelo presente certame;

1.14. Todos os itens devem comportar atualização, instalação e suporte para o período contratado.

1.15. Todos os produtos e serviços deverão ser orçados para um período mínimo de contrato de 36 meses.

ITEM 1 - LICENCIAMENTO DE USO DE SOFTWARE DE SOLUÇÃO DE SEGURANÇA UTM COM DESEMPENHO DE FIREWALL DE 20 GBPS COM SUPORTE, INSTALAÇÃO E TREINAMENTO.

1.16. Ser licenciado seu uso para permitir o desempenho de 20 Gbps pelo período de 36 meses;

1.17. Não limitar o quantitativo de canais VPN site-to-site simultâneos;

1.18. Não limitar o quantitativo de conexões VPN client-to-site;

1.19. Possuir manual de usuário completo, ajuda on-line, interface de administração e demais documentos correlatos em português;

1.20. Possuir sistema operacional customizado especificamente para funções de UTM. Não serão aceitos sistemas de firewall que sejam executados sobre sistemas operacional em versões ou configurações distribuídas comumente no mercado, como o Novell NetWare, Microsoft Windows, Linux ou FreeBSD;

1.21. Deve permitir a instalação em servidores físicos e em sistemas de virtualização como VMware, ou Microsoft Hyper-V.

RECURSOS GERAIS DO SOFTWARE

1.22. Deve suportar tecnologia de Firewall Stateful Packet Inspection;

1.23. Possuir conexão entre a estação de gerência e Appliance no modo criptografado tanto em interface gráfica, quanto em CLI (linha de comando). O Acesso a interface de administração deve ser via WEB sob o protocolo HTTPS com ergonomia voltada a usabilidade;

1.24. Gerenciamento do tráfego e estatísticas sumarizadas através de um painel de controle;

1.25. Possuir sistemas de alertas e notificações do sistema em tempo real na interface WEB e envios automáticos por e-mail;

1.26. Interface responsiva compatível com dispositivos móveis;

1.27. Interface em português e inglês;

1.28. O sistema deve permitir o acesso à interface de gerenciamento WEB por qualquer interface de rede configurada;

1.29. Permitir a criação de perfis de administração baseado em ACL (Acess List), de forma a possibilitar a definição de diversos administradores para o dispositivo, cada um responsável por determinada tarefa da administração;

1.30. Permitir a conexão simultânea de vários administradores, com poderes de alteração de configurações e/ou apenas de visualização das mesmas;

1.31. Permitir criar as definições de ACL (Acess List) completa por administrador, sendo possível especificar os direitos, como: somente Visualizar ou Editar "Alterar, Excluir, Cadastrar";

1.32. Permitir auditoria do sistema com log das ações dos administradores por tipo de recurso e período;

1.33. Possuir porta console para possíveis manutenções no produto;

1.34. Acesso via WEB a console shell para gerenciamento através de interface de linha de comando CLI (Command Line Interface). Configurações básicas via interface CLI como suporte a comandos para debug deverão ser suportadas por esta interface;

1.35. A interface CLI deve suportar a configuração de roteamento dinâmico no mínimo para os protocolos BGP, OSPF, RIP1 e RIP2 com suporte a interface Vty;

1.36. Possuir um Certificado digital (CA - Certificado de Autoridade) padrão X.509, nativo com chaves de 2048 bits, para os processos de autenticação do usuário, utilização do proxy SSL e em todas as conexões de serviços com o Appliance.

1.37. A solução deve manter um canal de comunicação segura, com criptografia baseada em certificados entre todos os componentes que fazem parte da solução de firewall, gerência, armazenamento de logs e emissão de relatórios;

1.38. Permitir a integração com qualquer autoridade certificadora válida emissora de certificados X509 que deve

seguir os padrões descritos na RFC 2459.

1.39. Capacidade para criação de objetos com a finalidade de facilitar a administração e configuração do sistema, deve atender no mínimo os seguintes tipos de objetos: endereço IP, endereço MAC, Portas de serviços e protocolos, atendendo no mínimo os seguintes protocolos (TCP, UDP, ICMP, IGMP, AH, EGP, ESP, GRE, RSVP, e SCTP), tabela de horário, período com especificação de data/hora inicial e final, tabela de palavras chaves com a possibilidade de especificar expressões regulares, tipos de conteúdo de arquivos (content types);

1.40. Possuir um sistema de armazenamento remoto com suporte a conexões do tipo SMB, NFS e Disco (USB-HDD);

1.41. Possuir mecanismo que permita a realização de cópias de segurança (backups) do sistema e restauração remota, através da interface gráfica, a solução deve permitir o agendamento diário ou semanal;

1.42. As cópias de segurança (backups) devem ser armazenadas em dispositivos remotos do tipo NFS (Network File System) ou Disco externo (USB-HDD);

1.43. O sistema deve permitir configurar o período ou número de cópias que deseja manter no repositório remoto e executar a manutenção de período automaticamente.

1.44. As cópias de segurança devem ser salvas compactadas e criptografadas de forma a garantir segurança, confiabilidade e confidencialidade dos arquivos de backup;

1.45. O sistema ainda deve contemplar um recurso de cópia de segurança do tipo snapshot, que contemple a cópia completa das configurações dos serviços e recursos do sistema;

1.46. Deve possibilitar a restauração do snapshot através da interface web de qualquer ponto remoto, de modo a contribuir para uma restauração imediata sem a necessidade de reinicialização do sistema;

1.47. Suporte e integração com servidores de Network Time Protocol (NTP) para atualização de data e hora do sistema, o que padroniza e evita problemas com o horário de verão;

1.48. Atualização automática do sistema para correções e releases. O sistema de atualização deve permitir agendamento para verificação diária da base de atualizações do fabricante.

1.49. As atualizações devem ser disponibilizadas no intervalo máximo de 15 dias. Não podendo ultrapassar este período;

1.50. Permitir desabilitar update automático;

1.51. Efetuar controle de tráfego e monitor por estado de conexão no mínimo para os seguintes protocolos (TCP, UDP, ICMP, IGMP, AH, EGP, ESP, GRE, RSVP e SCTP) baseados nos endereços de origem, destino e porta;

1.52. Suportar o Internet Protocol Versões 4 (IPv4);

1.53. Suporte à Interfaces Ethernet;

1.54. Suportar o protocolo 802.1q, para uso e segmentação da rede com VLANs;

1.55. Suportar o protocolo 802.1x, para autenticação RADIUS;

1.56. Suporte a interfaces do tipo MACVLAN;

1.57. Suportar o protocolo 802,1ax e 802.3ad (LACP), Link Aggregation Control Protocol;

1.58. Suporte à interfaces DSL;

1.59. Suporte à roteamento estático;

1.60. Suporte ao protocolo SNMP;

1.61. A solução deve suportar no mínimo o funcionamento com 2 (dois) equipamentos idênticos, de forma que funcione com tolerância a falhas (ativo/passivo);

AUTENTICAÇÃO

1.62. Suporte à múltiplos domínios de autenticação, mínimo 3(três) domínios;

1.63. Permitir o cadastro dos usuários e grupos em base de dados própria por meio da interface de administração WEB do dispositivo;

1.64. Suporte à sincronismo de usuários e grupos com servidores Windows AD® e Servidores LDAP;

1.65. Permitir a utilização de LDAP, LDAP/SSL para a autenticação de usuários;

1.66. Permitir a utilização de autenticação RADIUS para sincronismo de contas e sessões;

1.67. Permitir o login de usuários de forma transparente ao efetuar logon na rede para plataformas Windows 2008 e 2012 Servers (sem a necessidade de o usuário digitar novamente a senha), para todos os serviços suportados, considerando assim a autenticação do usuário, como uma autenticação unificada entre a plataforma Windows e o Appliance Firewall NG UTM;

1.68. Permitir o controle de acesso por usuário, para todas as plataformas com browser através de autenticação via portal WEB para todos os serviços suportados, de forma que um determinado usuário tenha seu perfil de acesso automaticamente carregado;

1.69. Possuir suporte a um sistema de autenticação do tipo Captive Portal capaz de redirecionar de forma automática a autenticação, deve ser compatível com autenticação Windows AD®, LDAP, RADIUS e LOCAL;

1.70. O Captive Portal deve suportar o protocolo HTTPS para a tela de autenticação do usuário e para administração dos serviços de Captive Portal para o usuário;

1.71. A solução deve permitir em seu portal de autenticação o cadastro de novos usuários, permitindo controle por área, para usuários convidados o Captive Portal solicitará informações para cadastro no sistema, enquadrando automaticamente à um perfil de acesso previamente configurado;

1.72. O sistema de Captive Portal deve ser capaz de aplicar uma política geral e gerenciar a sessão do usuário autenticado:

1.73. Controlar o número de sessões concorrentes por usuário;

1.74. Controlar o número de tentativas de autenticação não autorizada;

1.75. Bloquear o endereço IP de origem das tentativas de autenticação não autorizada;

1.76. Definir o tempo de bloqueio do endereço IP das tentativas de autenticação não autorizada;

1.77. Definir tempo de sessão por inatividade;

1.78. Identificar endereço IP;

1.79. Identificar endereço MAC;

1.80. Permitir o administrador efetuar logout de sessão de qualquer usuário através da interface de gerenciamento WEB da solução de firewall;

1.81. Os usuários devem ter acesso à alguns recursos tais como: alterar dados pessoais; alterar senha para os casos de usuário do tipo local; fazer o download do Certificado de Autoridade (CA) e acesso ao Termos de Uso;

SEGURANÇA

1.82. Prover a condição de configuração de uma Política padrão por agrupamento de devices ou zonas de rede, determinando origem e destino por tipo de agrupamento;

1.83. Possibilitar exigir autenticação para a política padrão;

1.84. Capacidade para trabalhar com conversão de endereços e portas (NAT/NAPT) conforme RFC 3022; ser capaz de aplicar mascaramento de pacotes do tipo: SNAT (source nat) por endereço IP de origem; SNAT (masquerade) por device de origem; DNAT (dnat) mascaramento de destino por endereço IP/porta de destino e Nat-T em VPN IPSec;

1.85. Prover mecanismos de segurança configuráveis, que permita habilitar proteção contra ataques do tipo: "Denied of Service; Portscan; Pacotes inválidos; SYN Flood; ICMP Flood";

1.86. Possuir mecanismo que permita habilitar e desabilitar recursos do tipo: "ICMP Echo/Request - ping; ICMP Redirect; ICMP Broadcast; Source Routing; Checksum; Log Inválidos; TCP be liberal";

1.87. Possuir mecanismo de configuração para o controle de tipos de conexão possibilitando definir limites máximos para cada tipo de controle das conexões do protocolo TCP;

1.88. Possuir mecanismo de configuração para o controle de conexão possibilitando definir limites de timeout para as conexões genéricas;

1.89. Possuir mecanismo de configuração para o controle de conexão do protocolo ICMP possibilitando definir limites de timeout;

1.90. Possuir mecanismo de configuração para o controle de conexão do protocolo UDP possibilitando definir limites de timeout;

1.91. Detectar automaticamente e inserir regras de bloqueio temporárias para varreduras de portas efetuadas contra o dispositivo ou contra qualquer máquina protegida por esse, mesmo que realizados em períodos maiores que 1 (um) dia;

1.92. Possuir politicas padrões de entrada para os serviços nativos do firewall, por agrupamento de device ou zonas de rede, podendo exigir ou não autenticação, com possibilidade de aplicar ações de bloqueio, permissão, inspeção IPS ou inspeção ATP;

1.93. Permitir definir as políticas de entrada para os serviços nativos do firewall, podendo aplicar filtros no acesso por: usuário, grupos, endereço IP de origem, endereço IP de destino e horário;

QOS

1.94. Deve permitir especializar as redes de forma a melhorar sensivelmente a qualidade de conexão, tratando de forma diferenciada e especifica as transmissões que exijam maior e melhor qualidade da rede;

1.95. Deve possuir mecanismo que permita criar controles por fila de prioridade, mínima de 5(cinco) níveis;

1.96. Deve ser capaz de alterar a velocidade dos acessos por nível de prioridade;

1.97. Deve ser capaz de criar limites de banda máxima por fila de prioridade;

1.98. Deve ser capaz de criar garantia de banda mínima por fila de prioridade;

1.99. Deve permitir a habilitação do controle de velocidade permitindo especificar a largura de banda ou velocidade Downstream e Upstream de cada barramento ou device;

1.100. Priorização de pacotes com suporte às tecnologias de tratamento ToS (Type of Service) e DSCP (DiffServ Code Point);

1.101. Permitir modificação de valores ToS para a priorização de roteamento dos pacotes;

1.102. Implementar no mínimo 5(cinco) níveis de roteamento e tipos de serviços, com configuração e marcação para códigos ToS através da interface gráfica;

1.103. Permitir modificação de valores DSCP dos pacotes para o DiffServ;

1.104. Implementar no mínimo 20 (vinte) classes de serviço distintas, com configuração do mapeamento e marcação para códigos DSCP através da interface gráfica;

BALANCEAMENTO DE LINK

1.105. Deve ser capaz de segmentar e priorizar o tráfego através das interfaces de rede;

1.106. Deve contemplar a função de roteamento por prioridade de links;

1.107. Deve ser "tolerante à falhas", ou seja, possuir recurso de FailOver;

1.108. Deve possuir mecanismos de controle de falhas de link, capaz de aplicar testes da disponibilidade em tempo real. Estes testes devem retornar para o sistema o status atual de cada link e em caso de falhas do link principal, este recurso deverá alterar o "gateway padrão" do sistema para o próximo link da lista de prioridades de links;

1.109. O serviço de FailOver de links deve possibilitar que os testes e monitoramento sejam realizados através do protocolo ICMP para endereços de hosts externos;

1.110. O monitoramento no protocolo ICMP deve permitir inserir múltiplos endereços para verificação e o link principal somente será marcado como inativo se todos os hosts externos pararem de responder;

1.111. Deve possuir as seguintes opções de configurações para o monitoramento do link que fazem parte do FailOver e Balanceamento de link:

1.112. Intervalo de monitoramento;

1.113. Quantidade tentativas de testes por host ou número de falhas necessárias antes de marcar o link como inativo;

1.114. Permitir utilizar um link como principal e outro como secundário. O tráfego apenas será redirecionado (FailOver) quando o principal ficar indisponível, retornado ao estado anterior quando o principal ficar ativo novamente;

1.115. Deve suportar regras de roteamento dos serviços de saída do próprio dispositivo de firewall, podendo

selecionar entre os links, inclusive definindo prioridade do tráfego;

1.116. Suportar o uso simultâneo de múltiplos links em um mesmo firewall, de provedores distintos ou não.

1.117. Permitir o balanceamento de links, inclusive com IPs dinâmicos para ADSL ou outra tecnologia de banda larga que não utilize IP Fixo;

1.118. Deve contemplar o recurso de balanceamento de links por políticas de segurança; podendo ser aplicadas por: origem, destino, conteúdo web, horário ou período de data e hora inicial e final, controles de tipo de conteúdo, tipo de pacote; políticas de mascaramento; políticas de proxy; usuário e grupos;

POLÍTICAS DE SEGURANÇA DO FIREWALL

1.119. O sistema deve integrar os respectivos recursos e serviços de integração com o firewall: NAT, proxy; filtro de conteúdo web, filtro de aplicações web, QoS, FailOver e balanceamento de links, de acordo as especificações técnicas descritas a fim de propiciar um sistema capaz de tratar o tráfego da rede em camadas, garantindo a segurança dos dados;

1.120. Estes recursos integrados devem permitir o tratamento do tráfego em camadas, de modo granular com o suporte a interceptar o tráfego SSL, identificar malwares e ações mal-intencionadas que utilizam o protocolo HTTPS para burlar firewalls, o sistema deve interceptar estas conexões, analisar e enviar os pacotes para tomadas de ações;

1.121. Deve também permitir a inspeção destes pacotes, detectar e prevenir dos ataques de intrusos, operando em conjunto com o firewall, impedir que acessos externos e/ou remotos executem rotinas de invasão. Executando ação pró ativa de bloqueio dos ataques;

1.122. Deve permitir gerar políticas de segurança capaz de filtrar os pacotes, integrar aos recursos de tratamento de filtro de conteúdo, filtro de aplicações, gerenciamento e controle dos pacotes definindo controle de banda por níveis de velocidade e garantia de banda por prioridade.

1.123. Deve permitir o roteamento estático por device, por endereço IP, serviços, usuários, grupos de usuários, para cada link de internet podendo distribuir o balanceamento de carga entre múltiplos links de internet ou ainda definir um roteamento exclusivo sem a opção de redundância ou FailOver;

1.124. As políticas de segurança devem permitir integrar em uma mesma interface interativa a definição de uma única política que atenda todos os recursos integrados com o firewall;

1.125. As políticas de segurança devem tomar ações do tipo: permitir, bloquear e inspecionar para o tráfego IPS ou Inspecionar para o tráfego ATP;

1.126. As políticas de segurança devem atender as especificações por prioridade, se o conteúdo do tráfego se enquadrar as definições da política, a mesma deve ser aplicada ignorando as políticas de menor prioridade;

1.127. Deve permitir o agrupamento de políticas respeitando as regras de negócio;

1.128. Deve permitir reordenação sempre que necessário;

1.129. Deve suportar mecanismos de balanceamento de links por política, inclusive com devices do tipo VLAN ou MACVLAN (endereços virtuais);

1.130. Deve ser permitido desabilitar uma política de segurança sem que seja necessário remove-la da lista;

1.131. A interação da interface ainda deve prover um recurso ou mecanismo para expandir a política, ou seja, permitir a visualização com as informações de filtros e a ação que compõe a regra;

VPN IPSEC

1.132. A solução deve prover comunicação através de túneis VPN "Virtual Private Network" ou "Rede virtual Privada". Ter como principal finalidade utilizar os recursos da rede pública "Internet" para conectar redes remotas.

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

1.134. Deve suportar VPN IPSEC Túnel site to site ou site to client;

1.135. Deve suportar VPN IPSEC RAS - Acesso remoto IPSEC;

1.136. Deve suportar os protocolos padrões de VPN: IPSEC, ESP, IKE e IKE versão 2;

1.137. A solução de VPN deve operar o padrão IPSEC, de acordo com as RFCs 2401 a 2412, de modo a estabelecer canais de criptografia com outros produtos que também suportem tal padrão;
1.138. O suporte aos protocolos e algoritmos de autenticação e integridade IKEv1 e IKEv2 de acordo a RFC 7296, de modo a estabelecer canais de autenticação e criptografia com outros produtos que suportem tal padrão;
1.139. Deve possuir suporte a algoritmos de criptografia IKE: 3DES, AES, Blowfish;
1.140. Deve possuir suporte a algoritmos de integridade IKE: md5, sha1, sha256, sha384 e sha512;
1.141. Deve possuir suporte a algoritmos de criptografia ESP: DES, AES, Blowfish e Camélia;
1.142. Deve possuir suporte a algoritmos de integridade ESP: md5, sha1, sha256, sha384, sha512, aesxcbc e aescmac;
1.143. Suporte ao menos à 5 Diffie-Hellman distintos;
1.144. A solução deve atender a suporte IKEv2 com suporte a fragmentação, de acordo a RFC 7383;
1.145. Deve possuir funcionalidade que permita estabelecer túneis de VPN com Appliances da mesma solução ou outras soluções de VPN implementadas atrás de firewalls, através de encapsulamento UDP, de acordo a RFC 3947;
1.146. Implementar os esquemas de troca de chaves manual, para os protocolos IKE e IKEv2 através de chave compartilhada (Pré-Shared Key);
1.147. Suportar Main Mode e Aggressive mode em IKE v1;
1.148. Possuir funcionalidade Dead Peer Detection (DPD) ou similar;
1.149. Suportar VPN Redundante (Failover) reestabelecimento automático da VPN IPSEC sobre um segundo enlace caso haja falha no enlace principal);
1.150. Suporte a conexão por FQDN "Full Quality Domain Name";
1.151. Deve permitir habilitar, desabilitar os túneis de VPN IPSEC
1.152. A solução deve prover recursos de controle de conexão no tratamento do protocolo IKE que possibilite definir parâmetros dos tempos de vida das conexões e retransmissão e da autenticação IKE;
1.153. O sistema de VPN IPSEC RAS deve funcionar como um provedor de VPN para clientes, de modo a atribuir aos clientes endereços IPs não válidos, colocando-os, virtualmente, em uma rede local estendida;
1.154. No modo VPN IPSEC RAS deve ser possível configurar o endereço/range IP a ser atribuída a interface de rede virtual do cliente de VPN, bem como sua máscara de rede, endereços dos servidores DNS, endereço dos servidores WINS, rota default e rotas para sub-redes;
1.155. O modo VPN IPSEC RAS deve suportar autenticação integrada X-Auth (Integração Windows AD, PAM LDAP e base de autenticação local) para usuários do firewall;
1.156. Deve possuir mecanismos de autenticação com suporte a EAP (MSCHAP2) para clientes VPN IPSEC Windows;
1.157. Compatibilidade com clientes VPN nativos para os sistemas operacionais iOS 7 ou superior, Android 4.4.4 ou superior, MacOS X 10.6 ou superior, Linux 2.6.36 ou superior, Windows 7 ou superior;

SERVIÇOS DE REDE (DDNS, DNS E DHCP)

1.158. A solução de UTM integrada deve permitir integração à serviços do tipo DDNS (Dynamic DNS);
1.159. Possuir suporte à publicação de hosts dinâmicos para os provedores de serviços: NO-IP e Dyndns;
1.160. Deve contemplar um mecanismo de atualização automática do DDNS por agendamento (update);
1.161. O serviço de DDNS deve ser compatível com Interface DSL ou PPOE;
1.162. O sistema também deve prover um recurso de redirecionamento DNS para provedores de DNS recursivo a fim de disponibilizar acesso a serviços de resolução de nomes remotos; permitir a consulta recursiva a partir dos redirecionamentos de DNS;
1.163. Permitir a configuração de acesso e redirecionamento por device de rede;
1.164. Suporte a cache de DNS;
1.165. Possuir mecanismos de proteção capaz de identificar ataques que disponibilizem servidores DNS válidos com autoridades sobre domínios configurados para responder um TTL (Time to live) muito baixo, inibindo a ação de guardar cache, o sistema deve possibilitar a proteção contra ataques que alteram a resposta a pesquisa de DNS para um

endereço IP dinâmico de servidores com códigos maliciosos;

1.166. O sistema de proteção a este tipo de resposta (pesquisa de domínios com TTL muito baixo) deve possuir a opção de exceção para endereços de hosts locais e por domínios possibilitando especificar hosts e domínios confiáveis que não queira guardar cache;

1.167. Deve permitir DNS Redirect por listas de hosts;

1.168. A solução de UTM integrada deve fornecer um serviço de DHCP (Dynamic Host Configuration Protocol) Server e DHCP Relay;

1.169. Deve possuir mecanismo de configuração e distribuição de pool de endereços IPs por device de rede, com suporte a interfaces do tipo ethernet, VLAN, inclusive interface MACVLAN (Virtuais);

1.170. Deve permitir a distribuição do pool de endereços IPs por filtro de grupo ou objeto de endereço MAC; permitir a distribuição de endereço IP fixado ao endereço MAC.

1.171. A distribuição dos dados de configurações de serviços de rede deve contemplar a distribuição de Gateway ou roteamento, a definição de um sufixo de DNS; lista de endereço de servidores de DNS e servidores Wins;

1.172. Deve permitir a definição do tempo de vida do DHCP para a renovação do endereço IP entregue;

ALTA DISPONIBILIDADE

1.173. A solução deve suportar funcionamento com 2 (dois) ou mais equipamentos idênticos, de forma que funcione com tolerância a falhas (ativo/passivo);

1.174. Os dois dispositivos devem ser ligados em paralelo, com réplicas das configurações entre eles. O dispositivo secundário não estará tratando o tráfego, ele entrará em funcionamento para tratamento de tráfego somente quando o dispositivo principal ficar inoperante;

1.175. Deverão ser capazes de manter o sincronismo de todos os itens de configuração e serviços, exemplo: Políticas de segurança, Configurações de segurança do firewall, Certificado de autoridade, Contas administrativas, Configuração de VPN, Configurações de rede, Roteamento estático, Roteamento dinâmico, Perfis, bases de antivírus, filtros web, IPS e ATP;

1.176. A alta disponibilidade deve ter persistência de sessão e detecção de falhas por protocolo VRRP;

1.177. O Sincronismo dos servidores deve ser por interface exclusiva;

RELATÓRIOS

1.178. A geração de relatórios deve ser centralizada e disponibilizada através da interface WEB da solução e disposta em um painel de controle de gerenciamento.

1.179. A geração dos relatórios detalhados deve ser opcional e configurável por tipo de relatório: proxy, ataques e ameaças, aplicativos e firewall;

1.180. A solução deve disponibilizar a geração de relatórios acessíveis, fáceis de usar e baseados na web que ofereça visão em tempo real, relatórios sumarizados, gráficos e históricos detalhados.

1.181. Os relatórios devem propiciar ao administrador base concreta de análise fornecendo uma visão profunda de como a rede e os computadores estão sendo utilizados, permitindo-se entender e reforçar quando necessário as regras de conformidade.

1.182. A solução também deve através da interface de administração web, permitir administradores visualizar os relatórios dos usuários.

1.183. Acesso centralizado e consistente a todos os logs sumarizados e eventos do sistema com a opção de verificação "Diária" e "Mensal" dos registros e ainda com a opção de extração no formato "PDF" e "CSV".

1.184. Suporte à geração em PDF para os relatórios estatísticos;

1.185. Deve ser capaz de gerar e manter os relatórios detalhados no mínimo por 7(sete) dias;

1.186. Deve suportar exportação dos relatórios detalhados no formato CSV;

1.187. Possuir um mecanismo de arquivamento dos relatórios gerados para download, o arquivamento deve ser mantido pelo período mínimo de 1(hum) mês;

1.188. Possuir um serviço de manutenção de limpeza dos registros de estatísticas e relatórios extraídos nos formatos CSV e PDF, mantendo os registros por um período mínimo de 30(trinta) dias;

1.189. A manutenção dos relatórios detalhados deve ser rotacional, automático e deve manter um período mínimo de 7 dias;

1.190. O sistema deve possuir um mecanismo de log que permita enviar os arquivos de log para outro servidor do tipo SYSLOG, especificando IP e porta;

1.191. Deve ser capaz de gerar relatório Online com (B.I) Business Intelligence para filtro na busca de relatórios;

1.192. Deve contemplar relação de eventos entre os itens de relatórios do proxy;

1.193. Deve contemplar relação de eventos entre os itens de relatórios das ameaças e aplicativos;

1.194. Deve contemplar os eventos de detecção do AntiMalware;

1.195. Deve contemplar relação de eventos entre os itens de relatórios dos atacantes;

1.196. A empresa fabricante da solução deve garantir que todos os relatórios detalhados devem ser assinados através de uma chave de integridade (key) que garanta a confiabilidade dos dados, atendendo ao Marco Civil nº 12.965/2014;

REGISTROS E LOGS DO SISTEMA

1.197. Deve atender os registros e logs do sistema das respectivas informações de gerenciamento por dispositivo: relatórios e gráficos gerais do sistema;

1.198. Gerar gráfico estatístico do sistema contendo informações do total de tráfego de rede e histórico diário por hora em (KB/ MB/ GB/ TB);

1.199. Gerar gráfico estatístico do sistema contendo informações do total de tráfego web via proxy e histórico diário por hora em (KB/ MB/ GB/ TB);

1.200. Gerar gráfico estatístico do sistema contendo informações do total de ameaças e aplicativos detectados pelo sistema de proteção de ameaças persistentes, tipo ATP e contemplar inclusive um histórico diário por hora em (KB/ MB/ GB/ TB);

1.201. Gerar gráfico estatístico do sistema contendo informações do total de ataques detectados pelo sistema de prevenção de intrusos, tipo IPS (Inspection Prevention System) e contemplar inclusive um histórico diário por hora em (KB/ MB/ GB/ TB);

1.202. Gerar gráfico estatístico do sistema contendo informações do total de tráfego de rede e histórico mensal por dia em (KB/ MB/ GB/ TB);

1.203. Gerar gráfico estatístico do sistema contendo informações do total de tráfego web via proxy e histórico mensal por dia em (KB/ MB/ GB/ TB);

1.204. Gerar gráfico estatístico do sistema contendo informações do total de ameaças e aplicativos detectados pelo ATP (Advanced Threats Protection) e histórico mensal por dia em (KB/ MB/ GB/ TB);

1.205. Gerar gráfico estatístico do sistema contendo informações do total de ataques detectados pelo IPS (Inspection Prevention System) e histórico mensal por dia em (KB/ MB/ GB/ TB);

1.206. Gerar histórico dos top 10 (dez) com o total do tráfego de rede em (KB/ MB/ GB/ TB) por: usuários, grupos, serviços/protocolos; regras de conformidade e categorias web;

1.207. Gerar histórico dos top 10 (dez) alertas de segurança dos ataques detectados pelo firewall com o total de hits;

1.208. Gerar histórico dos top 10 (dez) aplicativos web (ATP) com o total de hits;

1.209. Gerar histórico das top 10 (dez) ameaças APT (Advanced Persistent Threats) detectados pelo ATP com o total de hits e classificação do tipo de impacto na rede;

1.210. Gerar histórico dos top 10 (dez) ataques detectados pelo (IPS) com o total de hits e classificação do tipo de impacto na rede;

1.211. Gerar gráfico estatístico do sistema contendo informações de desempenho como: (%) percentual de uso de processamento (CPU), (%) percentual de entrada/saída (I/O), (%) percentual de carga média (LOAD), (%) percentual de utilização de disco e (%) percentual de consumo de memória (RAM);

1.212. Gráfico estatístico do consumo de banda, mínimo de 5 (cinco) níveis de prioridade em (B/ KB/ MB/ GB/ TB/);
1.213. Gráfico estatístico em tempo real do tráfego total da rede (RX/ TX);
1.214. Gráfico estatístico do sistema contendo histórico sobre o tráfego dos devices de rede (RX/ TX) e um serviço de monitoração em tempo real para cada device de rede;
1.215. A solução deve possuir um sistema de monitoração de tráfego para as novas conexões, podendo aplicar filtros por: endereço IP de origem, endereço IP de destino, serviços com a especificação de porta e protocolo. O serviço de monitoração deve retornar os dados especificados nos filtros e a respectiva regra de conformidade;
1.216. A solução deve possuir um sistema de monitoração de tráfego para as conexões estabelecidas, podendo aplicar filtros por: endereço IP de origem, endereço IP de destino, serviços com a especificação de porta e protocolo, inclusive limitando o quadro de respostas até 10 (dez) conexões estabelecidas. O serviço de monitoração deve retornar os dados especificados nos filtros, o total de tráfego em (KB/ MB/ GB/ TB), a velocidade em (bps/ kbps/ Mbps/ Gbps/ Tbps) e o número de pacotes trafegados;

RELATÓRIOS E GRÁFICOS GERAIS DO TRÁFEGO WEB VIA PROXY

1.217. Gerar gráficos estatísticos do tráfego WEB via Proxy contendo as seguintes informações: total das requisições, total das requisições bloqueadas;
1.218. Gerar gráfico, histórico ou resumo diário, da relação de eventos entre o total de trafego web via proxy dos acessos permitidos e os acessos bloqueados no intervalo de tempo de 1 (uma) hora;
1.219. Gerar gráfico, histórico ou resumo mensal, da relação de eventos entre o total de tráfego web via proxy dos acessos permitidos e os acessos bloqueados no intervalo de tempo de 1 (uma) hora;
1.220. Gerar gráfico, histórico ou resumo diário, da relação de eventos entre o total de trafego web via proxy dos acessos direto e os acessos ao cache no intervalo de tempo de 1 (uma) hora;
1.221. Gerar gráfico ou resumo mensal do total da relação de eventos entre o tráfego web via proxy dos acessos direto e os acessos ao cache no intervalo de tempo de 1 (hum) dia;
1.222. Gerar histórico dos Top Level 10 (dez) com o total do tráfego em (KB/ MB/ GB/ TB) e o total dos acessos, com a opção de ordenação por tráfego e por acessos, das regras de conformidade permitidas e tipos de conteúdo permitidos;
1.223. Gerar histórico dos Top Level 10 (dez) com o total do tráfego em (KB/ MB/ GB/ TB), tempo em (horas/ minutos) e total de acessos, com a opção de ordenação por tráfego, por tempo, e por acessos, das categorias permitidas e aplicativos permitidos;
1.224. Gerar histórico dos Top Level 10 (dez) "usuários" com o total do tráfego em (KB/ MB/ GB/ TB), tempo em (horas/ minutos), velocidade em (bps, Kbps/ Mbps/ Gbps/ Tbps), total de acessos permitidos e total de acessos bloqueados, com a opção de ordenação por tráfego, por tempo, permitidos e bloqueados;
1.225. Gerar histórico dos Top Level dos 10 (dez), inclusive a relação de eventos entre "usuários" e as "categorias web" com o total do tráfego em (KB/ MB/ GB/ TB), tempo em (horas/ minutos), Velocidade em (bps, Kbps/ Mbps/ Gbps/ Tbps), total de acessos permitidos e total de acessos bloqueados, com a opção de ordenação por tráfego, por tempo, permitidos e bloqueados;
1.226. Gerar histórico dos Top Level 10 (dez), inclusive a relação de eventos entre os "usuários" e os "aplicativos web" com o total do tráfego em (KB/ MB/ GB/ TB), tempo em (horas/ minutos), Velocidade em (bps, Kbps/ Mbps/ Gbps/ Tbps), total de acessos permitidos e total de acessos bloqueados, com a opção de ordenação por tráfego, por tempo, permitidos e bloqueados;
1.227. Gerar histórico dos Top Level 10 (dez), dos "bloqueados" com o total das tentativas de acesso, das regras de conformidade bloqueadas, categorias bloqueadas, aplicativos web bloqueados e tipos de conteúdo bloqueados;
1.228. A solução deve possuir um sistema de monitoração da navegação WEB via Proxy em tempo real por filtro do tipo: servidor, origem (endereço IP ou usuário), URL de destino e porta de serviço. O serviço de monitoração deve retornar o tempo de tráfego em (hora/ minuto/ segundo), a origem (endereço IP ou usuário), o total de tráfego em (B/ KB/ MB/ GB/ TB), a velocidade em (bps/ Kbps/ Mbps/ Gbps/ Tbps) e a URL de destino;

EDITAL

RELATÓRIOS E GRÁFICOS GERAIS DO TRÁFEGO ATP

1.229. Gerar gráficos estatísticos do tráfego ATP contendo as seguintes informações: total de ameaças detectadas, total de ameaças bloqueadas, total de aplicativos detectados, total de aplicativos bloqueados;

1.230. Gerar gráfico, histórico ou resumo diário, da relação de eventos entre o total de trafego ATP das ameaças detectadas a as ameaças bloqueadas no intervalo de tempo de 1 (uma) hora;

1.231. Gerar gráfico, histórico ou resumo diário, da relação de eventos entre o total de trafego ATP dos aplicativos detectados e os aplicativos bloqueados no intervalo de tempo de 1 (uma) hora;

1.232. Gerar gráfico, histórico ou resumo mensal, da relação de eventos entre o total de trafego ATP das ameaças detectadas e as ameaças bloqueadas no intervalo de tempo de 1 (hum) dia;

1.233. Gerar gráfico, histórico ou resumo mensal, da relação de eventos entre o total de trafego ATP dos aplicativos detectados e os aplicativos bloqueados no intervalo de tempo de 1 (hum) dia;

1.234. Gerar gráficos estatísticos do tráfego ATP contendo as informações do total de ameaças e aplicativos detectados por grau de risco e impacto na rede, mínimo de 3 (três) tipos de graus de risco ou impacto;

1.235. Gerar históricos ou resumos diários do total de tráfego ATP das ameaças e aplicativos detectados por grau de risco e impacto na rede, mínimo de 3 (três) tipos de graus de impacto no intervalo de tempo de 1 (uma) hora;

1.236. Gerar históricos ou resumos mensais do total de tráfego ATP das ameaças e aplicativos detectados por grau de risco e impacto na rede, mínimo de 3 (três) tipos de graus de impacto no intervalo de tempo de 1 (hum) dia;

1.237. Gerar histórico do Top Level 10 (dez) "detectados", com o total de detecções e o tipo de impacto das ameaças e aplicativos;

1.238. Gerar histórico dos Top Level 10 (dez), inclusive a relação de eventos entre as "ameaças" e os "usuários" com o tipo de impacto, total de detecções e o total de bloqueados, com a opção de ordenação por detecções e bloqueados;

1.239. Gerar histórico dos Top Level 10 (dez), inclusive a relação de eventos entre os "aplicativos" e os "usuários" com o total de detecções e o total de bloqueados, com a opção de ordenação por detecção e bloqueados;

1.240. Gerar histórico dos Top Level 10 (dez) "bloqueados" com o total das detecções, das ameaças e aplicativos;

RELATÓRIO E GRÁFICOS GERIAS DO TRÁFEGO IPS

1.241. Gerar gráficos estatísticos do tráfego IPS contendo as seguintes informações: total de ataques detectados, total de ataques bloqueados;

1.242. Gerar gráfico, histórico ou resumo diário, do total de trafego IPS da relação de eventos entre os "ataques detectados" e os "ataques bloqueados" no intervalo de tempo de 1 (uma) hora;

1.243. Gerar gráfico, histórico ou resumo mensal, do total de trafego IPS da relação de eventos entre os "ataques detectados" e dos "ataques bloqueados" no intervalo de tempo de 1 (hum) dia;

1.244. Gerar gráficos estatísticos do tráfego IPS contendo as informações do total dos ataques detectados por grau de risco e impacto na rede, mínimo de 3 (três) tipos de graus de risco ou impacto;

1.245. Gerar gráficos, históricos ou resumos diários, do total de tráfego IPS dos ataques detectados por grau de risco e impacto na rede, mínimo de 3 (três) tipos de graus de impacto no intervalo de tempo de 1 (uma) hora;

1.246. Gerar gráficos, históricos ou resumos mensais, do total de tráfego IPS dos ataques detectados por grau de risco e impacto na rede, mínimo de 3 (três) tipos de graus de impacto no intervalo de tempo de 1 (hum) dia;

1.247. Gerar histórico dos Tops 10 (dez) "ataques detectados", com o total de detecções e o tipo de risco ou impacto na rede;

1.248. Gerar histórico dos Top Level 10 (dez), inclusive a relação de eventos entre os "ataques" e os "endereços IP ou usuários" com o tipo de risco ou impacto na rede, total de detecções e o total de bloqueados, com a opção de ordenação por detecções e bloqueados;

1.249. Gerar histórico dos Top Level 10 (dez), inclusive a relação de eventos entre o "grau de risco" e os "endereços IP ou usuários" com o total de detecções e o total de bloqueados, com a opção de ordenação por detecção e bloqueados;

1.250. Gerar histórico dos Tops Level 10 (dez), "categorias de ataques" com o total das detecções e total de

bloqueados, com a opção de detalhar a categoria e identificar os endereços IPs ou usuários atacantes;

MODULOS LICENCIADOS

PROXY

1.251. Possuir Proxy nativo para tráfego HTTP, HTTPS, versões 1.0 e 1.1, FTP;

1.252. Deve possibilitar a conexão de tráfego para outros serviços e que contemplem a conexão em proxys HTTP, tais como: XMPP, SIP, H323, SMTP, POP3, IMAP, RTSP, TELNET e outros;

1.253. Deve permitir a configuração para outras portas de serviços;

1.254. Deve permitir implementar proxy transparente para os protocolos HTTP e HTTPS, de forma a dispensar a configuração dos browsers dos dispositivos clientes para a utilização das características o serviço;

1.255. Deve permitir implementar proxy configurado para os protocolos HTTP, HTTPS, FTP e SOCKS;

1.256. Deve permitir o armazenamento em cache de conteúdo trafegado pelo protocolo HTTP e HTTPS;

1.257. Possuir sistema de cache interno, armazenando requisições WEB em disco local e memória;

1.258. Deve permitir a definição do tamanho mínimo dos objetos salvos em cache no disco;

1.259. Deve permitir a definição do tamanho máximo dos objetos salvos em cache em memória;

1.260. Deve atender a estrutura de navegação através de hierarquia de proxy com e sem autenticação;

1.261. Deve permitir operar sem interceptação SSL.

1.262. Possibilitar a integração com servidores de cache WEB externos;

1.263. Deve ser capaz de armazenar cache dinâmicos para as atualizações Microsoft Windows Update®;

1.264. Deve ser capaz de armazenar cache dinâmicos de streaming no mínimo para endereços do Youtube® e MSN Vídeos®;

1.265. Deve ter capacidade de armazenar em cache dinâmicos conteúdo do Facebook®, Google Maps® e Sourceforge Downloads®;

1.266. Deve possuir a capacidade de excluir URL's específicas do cache web, configurável por listas de palavras chaves com suporte inclusive a expressões regulares;

1.267. Deve ter suporte à integração com antivírus HTTP através de hierarquia de proxy;

1.268. Possuir mecanismos de integração à interceptação SSL com suporte a conexões de proxy transparente ou proxy configurado;

1.269. Ter a capacidade de análise de HTTP e HTTPS, pelo Antimalware se determinados tipos de arquivos baseados na extensão contém vírus antes de entregá-lo ao usuário e suportar ao menos 2 scanners;

1.270. Ter a capacidade de trabalhar como Anti-Virus de Gateway permitindo a análise de arquivos específicos por extensão;

1.271. Permitir o gerenciamento de quarentena de Malware;

1.272. Permitir realizar Filtro de Conteúdo por Autoridade Certificadora;

1.273. Permitir desabilitar interceptação de SSL por domínio;

SISTEMA DE PROTEÇÃO AVANÇADA CONTRA AMEAÇAS

1.274. Possuir sistema de proteção avançada contra ameaças (ATP) nativo;

1.275. O sistema de ATP deve monitorar e analisar o tráfego da rede, identificar aplicativos e ameaças de ataques direcionados e persistentes e efetuar os respectivos bloqueios.

1.276. Deve ser baseado em uma lista de assinaturas eletrônicas que atue em tempo real analisando a camada de aplicação, capaz de identificar o conteúdo dos pacotes, fazer log (registros) das assinaturas trafegadas, inspecionar os pacotes e efetuar o descarte automático do pacote quando identificado assinaturas de pacotes maliciosos, inapropriados para o uso no ambiente corporativo;

1.277. A base de assinaturas do sistema de ATP nativo deverá ser fornecida pelo período do contrato;

1.278. A base de assinaturas deve possuir mínimo de 2(duas) modalidades de assinaturas, atendendo a identificação de ameaças e aplicativos;

1.279. Possuir um mínimo de 31 mil (trinta e um mil) assinaturas;

1.280. O fabricante deve garantir o fornecimento de atualizações regulares dentro do período de assinatura contratado;

1.281. Deve permitir a atualização automática das assinaturas por meio de agendamento diário;

1.282. Possuir capacidade de inspecionar e bloquear em tempo real, ameaças do tipo: activex, malware, malware-backdoors, ataques P2P, trojans, worms, user_agents, pua (adware, p2p, toolbars) malwares para mobile, blacklist, botcc, exploits-kits, file-executable, file-flash, file-identify, file-image, file-java, file-multimedia, file-office, file-other, file-pdf, games, inappropriate e vulnerabilidades conhecidas;

1.283. Possuir uma ferramenta de bloqueio de execução de aplicativos, integrado a base de Antivírus e Antimalware;

1.284. Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos do tipo: ads, cloud, colaboração, download, e-mail, games, mobile, p2p, proxy, remote, redes sociais; storage, streaming, update, voip e web.

1.285. Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos de VoIP tais como: Hotline, Asterisk, Linphone, SIP, Skype, Xlite SIP, X-Pro SIP, Cisco SIP, OpenSIP, Bria, ClearSea e Nero SIP;

1.286. Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos de Redes Sociais tais como: Aol Instant Messenger, Badoo, BaiduHi, Airtime, Blogger, BoldChat, ChatON, China.com, Facebook, Flickr, FC2, Fring, Google Analytics, Google App, ICQ, Linkdin, Meetup, MSM Messenger, Netlog, Skype, Tinder, Tuenti, Twitter, WhatssApp, WeChat e Zoho Chat;

1.287. Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos e transferências de arquivos do tipo P2P (peer to peer) tais como: BitTorrent, Gnutella, FastTrack, IceShare, Napster, Shareman e de Storages, tais como: Dropbox, Easy-share, Google Drive, Megashare, MegaUpload, Rapidshare, OneDrive, Yahoo Box, SoundCloud e Filemail, DivShare;

1.288. Possuir mecanismo de bloqueio para listas de reputação de endereço IP catalogadas no mínimo para 6(seis) categorias, capaz de permitir seleção por categorização, elas devem atender as seguintes classificações: spam, reputation, malware, attacks, anonymous e abuse;

1.289. Possuir mecanismo de bloqueio e proteção por localização GeoIP para uma lista mínima de 250 Países e Repúblicas;

1.290. Deve possuir mecanismos de integração nas conexões via proxy, a partir da interceptação SSL. Possuir capacidade de inspeção profunda de pacotes (Deep Package Inspection - DPI), conseguir inspecionar aplicações criptografadas incluindo todo o payload;

1.291. Suportar exceção de ameaças por assinatura; IP de origem ou IP de destino;

1.292. Suportar exceção de aplicativos por assinatura; IP de origem ou IP de destino;

1.293. Suportar exceção para base de reputação IP por endereço IP;

1.294. Suportar exceção para a base de localização GeoIp por endereço IP;

1.295. Ação de Bloqueio do pacote ou reset da conexão em tempo real;

1.296. Deve possuir mecanismos para gerar gráfico do histórico da relação de eventos entre as "ameaças detectadas" e as "ameaças bloqueadas";

1.297. Deve possuir mecanismos para gerar gráfico do histórico da relação de eventos entre os "aplicativos detectados" e os "aplicativos bloqueados";

1.298. Deve possuir mecanismos para gerar log dos registros das incidências, classificados em pelo menos 3 (três) níveis de impacto: "baixo; médio e alto";

1.299. Gerar registro do tipo Top Level, dos 10(dez) mais, inclusive da relação de eventos entre usuários e ameaças, usuário e aplicativos, aplicativos e ameaças identificados e bloqueados;

1.300. Todos os logs e registros devem permitir ser gerados por período: "diário ou mensal";

1.301. Possuir mecanismos para inspecionar, identificar e detectar os aplicativos e sub aplicativos trafegados via proxy e classificá-los de acordo com a base de assinaturas;

1.302. Possuir mecanismos para inspecionar, identificar e detectar as ameaças e ataques do tráfego geral, incluindo o

trafego via proxy e classificá-los de acordo com a base de assinaturas;

1.303. Deve permitir o bloqueio em caso de detecção dos aplicativos e ou ameaças e atacantes, com base nas políticas de cada assinatura;

SISTEMA DE PREVENÇÃO CONTRA INTRUSÃO

1.304. Possuir sistema de prevenção contra intrusão de atacantes (IPS) nativo;

1.305. O Sistema de IPS deve monitorar, analisar o trafego e proteger a rede contra ataques internos e externos e utilizar técnicas de varredura e identificação que filtrem e bloqueie os pacotes atacantes e descarte o pacote com conteúdo de código malicioso;

1.306. Deve ser baseado na identificação de assinaturas de tipos de ataques e aplicações com vulnerabilidades conhecidas. O IPS deve contemplar uma base de assinaturas capaz de identificar o método de ataque com base em modelos de comportamento, características dos protocolos de rede, sistemas operacionais, inclusive comandos executados e esse conjunto de informações deve permitir que o pacote malicioso seja identificado e bloqueado em tempo real pelo IPS.

1.307. Possuir pelo menos 18000 mil (dezoito mil) assinaturas;

1.308. O fabricante deve garantir o fornecimento de atualizações regulares dentro do período de assinatura contratado;

1.309. Deve permitir a atualização automática das assinaturas por meio de agendamento diário;

1.310. A base de assinaturas deve contemplar um mínimo de 65 (sessenta e cinco) categorias, atendendo a identificação de ameaças e atacantes;

1.311. A solução deve ser capaz de detectar e prevenir as seguintes ameaças: Exploits e vulnerabilidades específicas de clientes e servidores, mau uso de protocolos, comunicação outbound de malware, tentativas de tunneling, e ataques genéricos;

1.312. A solução deve prover mecanismos de proteção contra ataques dos serviços de rede e aplicações, protegendo pelo menos os seguintes serviços: aplicações web, serviços de, DNS, FTP, SNMP, Telnet, TFTP, serviços Windows (Microsoft Networking) e VoIP.

1.313. A solução deve prover mecanismos de proteção contra ataques as assinaturas relacionadas a web-server, IIS, Apache, MSSql, MySql para que seja usado para proteção específica de Servidores Web;

1.314. Deve possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias como Denial of Service (DoS), Exploits, Attack Response;

1.315. Detecção de ataques de RPC (Remote Procedure Call);

1.316. Deve prover mecanismos de Proteção contra ataques de SMTP (Simple Message Transfer Protocol) IMAP (Internet Message Access Protocol, Sendmail ou POP (Post Office Protocol);

1.317. Deve prover mecanismos de Proteção contra ataques de ICMP (Internet Control Message Protocol);

1.318. Deve possuir mecanismos de integração nas conexões via proxy, a partir da interceptação SSL. Possuir capacidade de inspeção profunda de pacotes (Deep Package Inspection - DPI), conseguir inspecionar pacotes criptografados incluindo todo o payload;

1.319. Suportar exceção de ameaças por assinatura; IP de origem ou IP de destino;

1.320. Ação de Bloqueio do pacote ou reset da conexão em tempo real;

1.321. Deve possuir mecanismo para gerar log dos registros das incidências, classificados em pelo menos 3 (três) níveis de impacto: "baixo; médio e alto";

1.322. Deve possuir mecanismos para gerar gráfico do histórico da relação de eventos entre os "ataques detectados" e os "ataques bloqueados";

1.323. Gerar registro do tipo Top Level, dos 10(dez) mais, inclusive da relação de eventos entre os tipos de ataques e usuários, os graus de impacto e usuários, ataques identificados e bloqueados;

1.324. Todos os logs e registros devem permitir ser gerados por período: "diário ou mensal";

1.325. Possuir mecanismos para inspecionar, identificar e detectar as ameaças e ataques do tráfego geral, incluindo o trafego via proxy, e classificá-lo de acordo a base de assinaturas;
1.326. Deve permitir o bloqueio em caso de detecção de ameaças e atacantes, com base nas políticas de cada assinatura;

CONTROLE DE APLICATIVOS WEB

1.327. O controle de aplicativos web deve possuir mecanismos de detecção capaz de tomar medidas contra o tráfego de rede indesejado por tipo de aplicativo e sub aplicativos em uso, deve ser baseado em decodificadores de assinaturas e protocolos.
1.328. O controle desses aplicativos devem permitir inspecionar, permitir ou bloquear estes acessos nas conexões HTTP e HTTPS através de proxy transparente ou proxy configurado, inclusive a definição de quais usuários, grupos de usuários, redes, devices ou agrupamentos de devices podem utilizar ou não estes recursos, definindo inclusive dentro das suas características quais recursos de cada aplicativo poderão ser utilizados.
1.329. A base deve contemplar um número mínimo de 790 aplicativos e sub aplicativos diferentes, catalogados e classificados em categorias, mínima de 24 categorias;
1.330. Possuir mecanismos de criação de regras que possibilite definir políticas de segurança de maneira simplificada, sem a necessidade de especificar endereço de origem ou destino das aplicações, para as tomadas de ação;
1.331. Reconhecer no mínimo aplicações do tipo redes sociais, aplicativos peer to peer, acesso remoto, games, streamings, aplicativos de lojas on line, mensageiros instantâneos, colaboração, vídeo conferência, e-mails, fóruns, bloggers, storage, proxy anônimos, antivírus entre outras;
1.332. Deve contemplar assinaturas que identifique pelo menos os aplicativos e sub aplicativos tais como: Youtube®, Facebook®, Twitter®, Linkedin®, Tumblr®, Bittorrent®, Gnutella®, AIM®, Baidu®, Syflex®, Logmein®, Join.me®, DropBox®, Onedrive®, Apple iCloud®, Amazon®, Ebay®, ITunnes®, Blospot®, Instagram®, Flickr®, Photoshop®, Picasso®, Myspace®, Netflix®, Justin TV®, Megavideo®, Skype®, Viber®, Whatsapp®, Yahoo Messenger®, Spotify®, Wunderlist®, Webex®, Gismodo®, Google News®, Google Docs®, Google Earth®, Google Translator®, Google Finance®, Money Control®, Morningstar®, Playstation®, Wii®, Xbox Live®;
1.333. Ser capaz de identificar assinaturas de aplicações de uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações de proxys que utilizam táticas evasivas via comunicações criptografadas, tais como Ultrasurf, Vtunnel, Zenguard, Privax, Proxydotorg;
1.334. O recurso deve de forma objetiva controlar aplicativos web 2.0 com a finalidade de melhorar o desempenho da rede e evitar improdutividade do grupo de usuários da rede;

FILTRO DE CONTEÚDO WEB

1.335. O filtro de conteúdo web deve possuir mecanismos de detecção capaz de tomar medidas contra o tráfego de rede indesejado dependendo da URL ou categoria web, deve ser baseado em uma lista de URL's classificadas por tipo de conteúdo;
1.336. O filtro de conteúdo web deve permitir inspecionar, permitir ou bloquear estes acessos nas conexões HTTP e HTTPS através de proxy transparente ou proxy configurado, inclusive a definição de quais usuários, grupos de usuários, redes, devices ou agrupamento de devices, podem acessar ou não as diversas categorias identificadas;
1.337. O filtro de conteúdo web deve possuir base de dados catalogada com mínimo de 40 milhões de URL's e classificada em no mínimo 80 categorias;
1.338. A solução deve possuir mecanismos de criação de regras que possibilite definir políticas de segurança de maneira simplificada, sem a necessidade de correlacionar endereços de origem e destino das URL's ou categorias web para as tomadas de ação;
1.339. A solução de filtro de conteúdo deve suportar a ação de forçar a pesquisa segura independente da configuração do navegador (browser) da estação de trabalho do usuário. Esta funcionalidade não permitirá que os sites de busca retornem resultados considerados inapropriados. Esta funcionalidade deve ser suportada no mínimo para os

buscadores "Google®", "Bing®" e "Yahoo®";

1.340. Deve possuir mecanismos de filtragem de métodos HTTP a fim de otimizar e melhorar a eficiência do tráfego web, deve comtemplar filtros do tipo: put, get, checkout, connect, delete, head, link, post, search e trace;

1.341. Deve permitir criar base de categorias personalizadas a partir de listas de URL's com suporte a lista de palavras chaves e expressões regulares;

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

1.343. Permitir a criação de filtros para arquivos e dados pré-definidos;

1.344. Os arquivos devem ser identificados por extensão e assinaturas;

1.345. Suporte a identificação de arquivos compactados, executáveis, imagens e multimídias, a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

1.346. Deve oferecer a opção de bloquear controles ActiveX e Java Scripts que possam comprometer o acesso web dos usuários;

1.347. Deve oferecer a opção de cota de tempo em horas ou minutos de navegação web por dia;

1.348. Deve oferecer a opção de cota de tráfego em MB de navegação web por dia;

1.349. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, Compactados, Executáveis, ISOs e etc) identificados sobre aplicações (HTTP, HTTPS e FTP) inclusive oferecendo a opção de controle de tamanho máximo de download por navegação;

1.350. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, Compactados, Executáveis, ISOs, etc) identificados sobre aplicações (HTTP, HTTPS e FTP) inclusive oferecendo a opção de controle de tamanho máximo de upload por navegação;

1.351. Deve suportar mecanismos de filtro e controle de login no Google® por domínio, permitindo ao administrador especificar os domínios permitidos;

1.352. O sistema de filtro de conteúdo poderá ser aplicado por definição de horário ou período de validade do filtro; podendo ou não especificar usuários, grupos de usuários, rede ou agrupamento de device para todos os recursos de filtragem e controles estabelecidos;

VPN SSL

1.353. A solução deve prover comunicação através de VPN SSL que permita um usuário remoto devidamente autorizado a utilizar um navegador WEB moderno para acessar com segurança diversos serviços da rede privada;

1.354. A solução deve suportar acesso com chaves de criptografia com tamanho igual ou superior a 128 bits, de forma a possibilitar a criação de canais seguros ou VPNs através da Internet;

1.355. A VPN SSL deve possibilitar o acesso a toda infraestrutura de acordo com a política de segurança, através de um plug-in ActiveX e/ou Java;

1.356. O acesso deve oferecer versatilidade, facilidade de uso, e controles específicos de grupos e usuários em cada modalidade de aplicação e deve estar disponível através de um portal WEB.

1.357. Deve prover acesso via túnel SSL utilizando um navegador sem a necessidade de um cliente instalado na estação remota, e ser compatível com o navegador Mozilla Firefox versão 47;

1.358. Deve ser compatível com as plataformas operacionais: MS-Windows, Linux, MacOS;

1.359. Deve possuir mecanismos de tunelamento de aplicações através de um portal web, com suporte a desvio de porta (Port Forward) para as aplicações internas;

1.360. Permitir acesso interno e externo ao portal web;

1.361. Deve suportar as seguintes modalidades de aplicações: Aplicações Túnel do tipo cliente-servidor, Aplicações de acesso remoto tais como: VNC, SSH, Terminal Service, Aplicações web do tipo HTTP e HTTPS, Compartilhamento de rede do tipo SMB;

1.362. Deve possuir suporte a autenticação integrada X-Auth (Integração Windows AD, PAM LDAP e base de

autenticação local) para usuários do firewall;

DESCRIÇÃO DA INSTALAÇÃO, SUPORTE E ATUALIZAÇÃO

1.363. A CONTRATADA deverá realizar a instalação e configuração das licenças contratadas;

1.364. A instalação deve ser feita por técnicos treinados e certificados, comprovados através de atestado emitido pelo fabricante;

Toda a despesa de deslocamento e hospedagem deve ser de responsabilidade da contratada;

1.365. A CONTRATADA deve fornecer gerenciamento e suporte REMOTO para a solução de segurança em horário comercial (Segunda-feira a Sábado de 08h às 22h), pelo tempo de contrato, com as seguintes características: A contratada deve possuir serviço de abertura de chamados remoto capaz de abrir chamados de forma centralizada, em caso de ocorrências de defeitos e/ou falhas na rede relativos aos equipamentos e/ou produtos fornecidos;

1.366. A CONTRATADA deverá prestar suporte para criação de regras, configuração de módulos do UTM, auxilio na configuração de VPN e duvidas da contratante na operação do sistema;

1.367. A CONTRATADA deverá iniciar o atendimento de suporte em no máximo 8 horas úteis após a abertura do chamado;

1.368. A CONTRATADA será eximida da aplicação das sanções administrativas para os respectivos chamados em que sejam descumpridos os tempos de solução, desde que comprovadas as seguintes situações: Quando constatado que o problema está relacionado a "bug" no produto e que o fabricante não possui uma correção imediata para tal, sendo este fato declarado pelo próprio;

1.369. A CONTRATADA tomou todas as medidas possíveis visando providenciar solução de contorno;

1.370. A CONTRATADA deverá fornecer atualizações de software, incluindo novas versões, por um período mínimo de 36 meses.

DESCRIÇÃO DO TREINAMENTO PARA O SISTEMA DE FIREWALL UTM

1.371. Deverá ser fornecido treinamento para a solução de firewall adquirida (hardware ou software) para a equipe do cliente;

1.372. Carga Horária mínima de 30 horas;

1.373. O instrutor deverá ser certificado pela fabricante dos produtos para realizar os treinamentos, este deverá ser comprovado mediante apresentação de certificado expedido pela fabricante da solução de segurança da informação;

1.374. O material a ser fornecido no treinamento deverá ser o material certificado pelo próprio fabricante, não serão aceitas cópias de apostilas;

1.375. Toda a infraestrutura, os custos de material (apostilas, manuais, etc.), alimentação (coffee break), instrutor (deslocamento, hospedagem e vencimentos) ficará a cargo da CONTRATADA;

1.376. O treinamento deverá conter em seu conteúdo questões práticas e teóricas sobre o funcionamento e os recursos da solução proposta;

1.377. Deverá ser fornecido um 01 lanche (coffee break) para cada 4 horas de treinamento suficiente para todos os alunos;

1.378. Deve ser incluído, caso exista, módulos básicos e avançados de modo a cobrir todas as funcionalidades da solução ofertada;

1.379. Este treinamento poderá ser realizado em ambiente externo ao da CONTRATANTE, inclusive com os recursos para laboratórios (handson) salvo em caso de necessidade e acordo entre CONTRATADA e CONTRATANTE;

1.380. Os cursos deverão ser realizados em horários e data a serem acordados pela CONTRATADA e CONTRATANTE;

1.381. A CONTRATADA deverá ofertar as instalações na localidade da CONTRATANTE para a realização dos treinamentos com os requisitos mínimos de infraestrutura de sala de treinamento;

GARANTIA:

1.382. Toda solução deverá ser fornecida com suas respectivas licenças de funcionamento em sua capacidade total,

com garantia de 03 (três) anos;

1.383. Os equipamentos descritos nas Especificações Técnicas, deverão ter garantia mínima de 36 meses, contados a partir do aceite da fiscalização do contrato;

1.384. Durante o período de garantia, a(s) contratada(s) deverá(ão) disponibilizar um número de contato telefônico da cidade de Vitória (prefixo 027) ou DDG (0800) para abertura de chamado técnico, que deverá ser identificado por um número, por uma data e por uma hora, para que o mesmo possa ser devidamente acompanhado;

1.385. A contratada fornecerá, na data de assinatura do contrato, endereço eletrônico e número de fax para eventual contato que se faça necessário, no caso de indisponibilidade do acesso telefônico;

1.386. A impossibilidade de recebimento da abertura de chamado através de tentativa nos canais de atendimento informados não exime o fornecedor do prazo de manutenção;

1.387. A garantia será prestada na modalidade *on site* e deverá incluir os serviços de manutenção para resolução de problemas de hardware ou software, com substituição de peças ou equipamentos defeituosos, sem qualquer limitação quanto ao quantitativo das mesmas, por outros originais e em estado de novo, compatíveis com as características técnicas especificadas ou superiores, sem quaisquer ônus adicionais para a PMPK;

1.388. Durante o período da garantia do equipamento, a(s) CONTRATADA(s) deverá(ão) prover suporte telefônico para todo problema de hardware, software e configuração dos equipamentos

1.389. O início do atendimento deverá ser realizado em até 24 (vinte e quatro) horas após a abertura do chamado

1.390. As despesas relativas ao transporte de equipamentos, incluindo serviços de manutenção ou substituição, deverão correr por conta da CONTRATADA;

1.391. A fiscalização da PMPK será responsável pelo "ateste" na(s) Nota(s) Fiscal(is), acompanhamento da entregas dos equipamentos e assistência técnica na garantia;

1.392. A(s) CONTRATADA(s) deverá(ão) comunicar por escrito à fiscalização contratual, imediatamente, a impossibilidade de execução de qualquer obrigação contratual, para a adoção das providências cabíveis;

1.393. A falta de peças e/ou equipamentos não poderá ser alegada como motivo de força maior, e não exime a(s) CONTRATADA(s) das penalidades a que está(ão) sujeita(s) pelo não cumprimento dos prazos estabelecidos;

1.394. A(s) CONTRATADA(s) deverá(ão) fornecer correções automáticas das versões de software / firmware durante o período de garantia, caso seja detectado algum problema;

1.395. A(s) CONTRATADA(s) deverá(ão) garantir a total compatibilidade da solução proposta com novas implementações tecnológicas que vierem a ser desenvolvidas pelo fabricante do equipamento fornecido, visando assegurar a evolução e continuidade da base instalada;

1.396. Os empregados da CONTRATADA deverão trajar uniforme com logotipo da empresa e crachá de identificação, enquanto permanecerem nas dependências da CONTRATANTE;

1.397. A(s) CONTRATADA(s) assumirá(ão) inteira responsabilidade pela execução dos eventuais serviço no prazo de garantia, correndo por sua própria conta quaisquer ônus, encargos sociais, trabalhistas, previdenciários, tributos, taxas, licenças e férias, concernentes à contratação, inclusive seguros contra acidentes de trabalho, bem como o de indenizar todo e qualquer dano e prejuízo pessoal ou material que possa advir, direta ou indiretamente, no exercício de suas atividades;

1.398. Os serviços deverão ser executados com observância das especificações técnicas e regulamentação aplicável ao caso, com esmero e correção, refazendo tudo quanto for impugnado pela fiscalização, se necessário;

1.399. As despesas relativas aos eventuais deslocamentos do equipamento ou insumos deverão ocorrer integralmente por conta da(s) CONTRATADA(s), sem quaisquer ônus adicionais para o CONTRATANTE, durante todo o período de garantia;

1.400. Deverão ser obedecidas as normas de segurança e medicina do trabalho para esse tipo de atividade, ficando por conta da(s) CONTRATADA(s) o fornecimento, antes do início da execução dos serviços, dos Equipamentos de Proteção Individual - EPI, se necessário;

1.401. Indicar, na data de assinatura do contrato, nome e telefone de funcionário que atuará como preposto,

conforme preceitua o art. 68 da Lei 8666/93.

1.402. Observações:

1.403. Os prazos deste item poderão ser prorrogados mediante justificativa escrita da(s) CONTRATADA(s), submetida à apreciação do fiscal do CONTRATANTE.

DA ENTREGA E RECEBIMENTO DOS MATERIAIS

1.404. Os softwares, hardwares e serviços deverão ser entregues e instalados no prazo máximo indicado no cronograma abaixo (em dias úteis):

ID	Atividade	Duração
1	Fornecimento de Softwares e Hardware e Implantação da Solução.	Até 30 (trinta) dias após emissão das Autorizações de Fornecimento ou Ordens de Serviços.

1.405. Os softwares, hardwares deverão ser entregues no Almoxarifado Central da Prefeitura Municipal de Presidente Kennedy, no endereço: Avenida Orestes Baiense, S/N, Ao Lado do Posto de Saúde Willian Borges - Tel.: (028) 3535-1303, com todos os produtos e acessórios pertinentes e a Nota Fiscal correspondente;

1.406. O recebimento provisório será feito pelo Almoxarifado Central, supracitado, mediante recibo, não configurando aceite. Executado o objeto, será recebido na forma prevista no art. 73, incisos I e II, alínea "B" da Lei 8.666/93, após a conferência quantitativa e qualitativa devidamente atestada na Nota Fiscal correspondente, não excluindo a responsabilidade civil a ele relativa, nem a ético-profissional;

1.407. Os equipamentos deverão ser novos e sem uso. Não serão aceitos equipamentos usados, remanufaturados ou de demonstração;

1.408. Os equipamentos deverão ser entregues nas caixas lacradas pelo fabricante, não sendo aceitos equipamentos com caixas violadas;

1.409. Devem ainda estar em produção no mercado, não podendo configurar em listas de produto fora de linha até a data de recebimento provisório;

1.410. O CONTRATANTE poderá efetuar consulta dos números de série dos equipamentos junto ao fabricante, informando data de compra e empresa adquirente;

1.411. O aceite referente ao recebimento definitivo será processado em até 15 (quinze) dias úteis, contados da entrega da Nota Fiscal;

1.412. A(s) CONTRATADA(s), para fornecer os equipamentos, deverá(ão) disponibilizar um técnico responsável pela demonstração e comprovação do atendimento de todas as especificações técnicas descritas neste Termo de Referência.

1.413. Os testes deverão ser realizados no prazo estipulado no item anterior;

1.414. O atendimento a todos os requisitos técnicos é condicionante para o recebimento definitivo;

1.415. O CONTRATANTE também poderá efetuar consulta junto aos órgãos competentes para certificar a legalidade do processo de importação;

1.416. Em caso de importação dos produto, a(s) CONTRATADA(s) deverá(ão) comprovar a origem dos produtos importados e a quitação dos tributos de importação a eles referentes. Os referidos comprovantes deverão ser apresentados no momento da entrega do objeto;

1.417. Na execução dos serviços, a empresa CONTRATADA cumprirá todos os padrões de segurança e regras de uso e de controle de acesso às instalações da Prefeitura Municipal de Presidente Kennedy. A empresa CONTRATADA se compromete a manter sigilo acerca das informações obtidas e geradas no decorrer do trabalho;

1.418. Pertencerão exclusivamente a Prefeitura os direitos relativos aos produtos desenvolvidos e elaborados durante a vigência do Contrato, sendo vedada sua reprodução, transmissão e/ou divulgação sem o seu respectivo consentimento.

1.419. Caso não seja possível à entrega dos equipamentos citados neste termo a CONTRATADA deve fornecer um

equipamento de superior configuração.

OBRIGAÇÕES DA CONTRATADA

1.420. Indicar um preposto para o contrato, sendo este o interlocutor da CONTRATADA junto a PMPK para os assuntos relativos ao cumprimento das cláusulas contratuais e para participar de reuniões de acompanhamento, sempre que solicitado;

1.421. Responsabilizar-se técnica e administrativamente pelo objeto contratado, não sendo aceito, sob qualquer pretexto, a transferência de responsabilidade a outras entidades, sejam fabricantes, técnicos ou quaisquer outros;

1.422. A CONTRATADA responderá integralmente por perdas e danos que vier a causar a Prefeitura ou a terceiros em razão de ação ou omissão, dolosa ou culposa, sua ou dos seus prepostos, independentemente de outras combinações contratuais ou legais a que estiver sujeita;

1.423. Fornecer a seus técnicos todas as ferramentas, manuais e instrumentos necessários à execução dos serviços;

1.424. Submeter a relação dos técnicos credenciados a prestarem os serviços, devendo promover, de imediato, as substituições daqueles que, a critério da Prefeitura, venham a demonstrar conduta nociva ou incapacidade técnica;

1.425. O fornecedor não poderá cobrar valores adicionais ao valor do contrato, tais como custos de deslocamento, alimentação, transporte, alojamento, trabalho em sábados, domingos, feriados ou em horário noturno, bem como qualquer outro valor adicional.

OBRIGAÇÕES DA CONTRATANTE

1.426. Zelar pela segurança dos equipamentos, evitando o manuseio por pessoas não habilitadas;

1.427. Designar servidores como responsáveis, ficando os mesmos encarregados de manter atualizados os registros dos equipamentos em manutenção;

1.428. Documentar todas as implementações efetuadas, bem como atualizar em caso de mudanças no ambiente;

1.429. Designar a Gestão e Fiscalização do Contrato.

FISCALIZAÇÃO DO CONTRATO

1.430. A Fiscalização será exercida por um Servidor da Divisão de Tecnologia da Informação, a quem incumbirá acompanhar a execução dos serviços, determinando à CONTRATADA as providências necessárias ao regular e efetivo cumprimento do contrato;

1.431. A gestão e fiscalização do contrato deverão ser orientadas pelas condições estabelecidas no Art. 67 da Lei 8.666/93.

PRAZO DE VALIDADE DO CONTRATO

1.432. O prazo de validade do contrato será de 12 (doze) meses, contado a partir de sua assinatura.

PAGAMENTO

1.433. O(s) pagamento(s) à(s) Contratada(s) será(ão) efetuado(s) em até 30 (trinta) dias, a partir da data de emissão nota fiscal, sendo a nota fiscal sendo emitida após o aceite definitivo do equipamento, bem como da prestação dos serviços;

1.434. Fica a CONTRATADA ciente de que, quando da ocasião do pagamento, será verificado se as condições de habilitação estão mantidas.

DOTAÇÃO ORÇAMENTÁRIA

ÓRGÃO: 004 - SECRETARIA MUNICIPAL DE ADMINISTRAÇÃO

UNIDADE: 001 - SECRETARIA MUNICIPAL DE ADMINISTRAÇÃO

PROJETO ATIVIDADE: 004001041220083107 - AQUISIÇÃO DE LINK, IMPLANTAÇÃO E MANUTENÇÃO DA LOGÍSTICA DIGITAL NO MUNICÍPIO

33903900000 - OUTROS SERVIÇOS DE TERCEIROS - PESSOA JURIDICA - 15300000000 - TRANSFERENCIA DA UNIÃO

EDITAL

REFERENTE ROYALTIES DO PETROLEO.

PENALIDADES

1.435. No caso de descumprimento de obrigações contratuais, serão aplicadas sanções administrativas em conformidade com os Arts. 81, 86, 87 e 88 da Lei 8.666/93.

Leones Souza da Silva
Div. de Tecnologia da Informação

PREGÃO ELETRÔNICO Nº 000018/2020

OBJETO: **CONTRATAÇÃO EXCLUSIVA DE MICROEMPRESA OU EMPRESA DE PEQUENO PORTE PARA** LICENCIAMENTO DE USO DE SOFTWARE DE SOLUÇÃO DE SEGURANÇA UTM COM DESEMPENHO DE FIREWALL DE 20 GBPS COM SUPORTE, INSTALAÇÃO E TREINAMENTO.

Ítem	*Lote*	*Código*	*Especificação*	*Marca/Modelo*	*Unidade*	*Quantidade*	*Unitário*	*Valor Total*
00001	00001	00000980	**LICENCA DE USO ,** *LICENCIAMENTO DE USO DE SOFTWARE DE SOLUÇÃO DE SEGURANÇA UTM COM DESEMPENHO DE FIREWALL DE 20 GBPS COM SUPORTE, INSTALAÇÃO E TREINAMENTO.*		UND	1	34.451,66	

ANEXO III - MODELO DE DECLARAÇÃO CONJUNTA

MODELO DE DECLARAÇÃO CONJUNTA

PREGÃO ELETRÔNICO Nº 000018/2020

Em cumprimento ao disposto no edital de PREGÃO ELETRÔNICO N° 000018/2020 , a _____ (nome da empresa) com sede no endereço _____ (endereço completo), inscrita no CNPJ nº _____, por seu representante legal, Sr(a) _____, RG nº _____, CPF nº _____, DECLARA sob as penas da lei:

1 - Para fins do disposto no inciso V do art. 27 da Lei nº 8.666 de 21 de junho de 1993, acrescido pela Lei nº 9.854 de 27 de outubro de 1999, que não emprega menor de dezoito anos em trabalho noturno, perigoso ou insalubre e não emprega menor de dezesseis anos, ressalvando o emprego para menor, a partir de quatorze anos, na condição de aprendiz.

2 - Para fins de recebimento de tratamento favorecido e diferenciado nesse processo licitatório, que o seu enquadramento legal é de _____ (MICROEMPRESA, EMPRESA DE PEQUENO PORTE OU MICROEMPREENDEDOR INDIVIDUAL), pois cumpre os requisitos do artigo 3º da Lei Complementar nº 123/2006.

2.1 Declara sob as penas da Lei, que cumpre os requisitos legais para qualificação como Microempresa (ME) ou Empresa de Pequeno Porte (EPP), conforme art. 3º da Lei Complementar nº 123/2006 e que não está sujeita a quaisquer dos impedimentos do § 4º do referido artigo.

2.1.1 (Observação: em caso afirmativo assinalar a ressalva abaixo)
Declaramos possuir restrição fiscal no(s) documento(s) de habilitação e pretendemos utilizar o prazo previsto no art. 43, § 1º da Lei Complementar nº 123/2006 para a regularização, estando ciente que, do contrário, haverá decadência do direito à contratação, como também sujeição às sanções previstas no art. 81 da Lei nº 8.666/1993.

3 - Que, até a presente data, inexistem fatos impeditivos de sua habilitação no processo licitatório, estando ciente da obrigatoriedade de declarar ocorrências posteriores.

4 - Que tomou conhecimento dos aspectos relevantes que possam influir direta ou indiretamente na prestação do serviço, inclusive sobre a localidade onde serão executados os serviços.

5 - Que recebemos os documentos e tomamos conhecimento das condições locais da área destinada ao objeto da licitação em epígrafe.

6 - Que não se encontra inadimplente ou impedida de licitar, e nem é objeto de quaisquer restrições ou notas desabonadoras no Cadastro de Fornecedores, de quaisquer órgãos da Administração Pública direta ou indireta.

Município/UF, ____ de _____ de _____ .

_____
Representante legal da empresa

ANEXO IV - MODELO DE CONTRATO
MINUTA DE CONTRATO Nº ____/ 2020
REF. Pregão Eletrônico Nº 000018/2020
PROCESSO Nº 025567/2019

Contrato que entre si celebram o **MUNICÍPIO DE PRESIDENTE KENNEDY** e a empresa _____, na qualidade de CONTRATANTE e CONTRATADA, respectivamente, para o fim expresso nas cláusulas que o integram.

O **MUNICÍPIO DE PRESIDENTE KENNEDY, ESTADO DO ESPÍRITO SANTO**, pessoa jurídica de direito público interno, sediada à Rua Átila Vivácqua, 79 - centro - Presidente Kennedy/ES, inscrita no CNPJ sob o nº 27.165.703/0001-26, por meio de delegação conforme preceitua a Lei nº 1.356 de 5 de dezembro de 2017, por seu representante legal, o (a) Secretario (a) Municipal de _____, Sr (a). _____, brasileiro (a), residente e domiciliado à rua _____, ES, portador da Carteira de Identidade nº _____ e do CPF nº _____, doravante denominado CONTRATANTE e, de outro lado, a empresa _____ pessoa jurídica de direito privado, inscrita no CNPJ-MF sob o nº _____, com sede _____, por seu representante legal, Sr. _____, doravante denominada CONTRATADA, resolvem firmar o presente contrato, nos termos do procedimento licitatório, conforme Edital de Pregão Eletrônico nº 000018/2020, Processo nº 025567/2019, tudo de acordo com a Lei 10.520/2002, Decreto Municipal 115/2014 e Lei Federal nº 8.666/93 e alterações, que se regerá mediante as Cláusulas e condições que subseguem:

CLÁUSULA PRIMEIRA - Do Objeto
1.1 Constitui objeto do presente contrato a **CONTRATAÇÃO EXCLUSIVA DE MICROEMPRESA OU EMPRESA DE PEQUENO PORTE PARA** LICENCIAMENTO DE USO DE SOFTWARE DE SOLUÇÃO DE SEGURANÇA UTM COM DESEMPENHO DE FIREWALL DE 20 GBPS COM SUPORTE, INSTALAÇÃO E TREINAMENTO, em conformidade com as quantidades e especificações contidas no Edital que originou a presente contratação.

CLÁUSULA SEGUNDA - Dos Documentos Integrantes
2.1. Fazem parte integrante deste contrato todos os documentos e instruções, inclusive as propostas e Termo de Referência, que compõem o edital de licitação acima transcrito, completando o presente contrato para todos os fins de direito, independente de sua transcrição, obrigando-se as partes em todos os seus termos.

CLÁUSULA TERCEIRA - Do Prazo de Início e da Duração do Contrato
3.1. O presente Contrato terá duração até....., a contar da assinatura da ordem de fornecimento.

CLÁUSULA QUARTA - Do Preço e da Forma de Reajuste
4.1. Pelo objeto do contrato a(s) contratada(s), receberá(ao) a importância de R$ ..... (.....).
4.2. O preço do contrato é fixo e irreajustável, pelo período de 12 (doze) meses contados da data prevista para apresentação da proposta, de acordo com o art. 40, XI da Lei 8666/93 e art. 3º, § 1º da Lei 10.192/2001.
4.2.1. Em caso de prorrogação deste contrato, o índice de reajuste a ser utilizado será o Índice Nacional de Preços ao Consumidor Amplo - **IPCA**.
4.3. No preço já estão incluídos todos os custos e despesas, dentre eles, direitos trabalhistas, encargos sociais, seguros, transporte, embalagens, impostos, taxas, supervisão e quaisquer outros benefícios e custos, bem como demais despesas necessárias à perfeita conclusão do objeto licitado que porventura venham a incidir direta ou indiretamente sobre a prestação dos serviços.

CLÁUSULA QUINTA - Do Local e da Forma de Pagamento
5.1. Os pagamentos serão efetuados mediante a apresentação de documento fiscal hábil, sem emendas ou rasuras, relativo ao(s) material(ais) **efetivamente** entregue(s). Os documentos fiscais, depois de conferidos e visados, serão encaminhados para processamento e pagamento em até 30 (trinta) dias, após a sua apresentação.
5.2. O contratado deverá apresentar ainda os comprovantes de quitação dos encargos especificados no Edital.

5.3. Ocorrendo erros na apresentação do documento fiscal, o mesmo será devolvido à CONTRATADA para correção, ficando estabelecido que o prazo para pagamento será contado a partir da data de apresentação da nova fatura, devidamente corrigida.

5.4. Poderá deduzir do pagamento importâncias que a qualquer título lhe forem devidas pela CONTRATADA, em decorrência de inadimplemento contratual.

5.5. O pagamento das faturas somente será feito em carteira ou cobrança simples, sendo expressamente vedada à CONTRATADA a cobrança ou desconto de duplicatas através da rede bancária ou de terceiros.

5.6. Somente após haver sanado as falhas e/ou irregularidades apontadas, a CONTRATADA será considerada apta para o recebimento do pagamento correspondente.

5.7. O PAGAMENTO SOMENTE SERÁ EFETUADO nos termos definidos pela Instrução Normativa SFI n° 001/2013, aprovada pelo Decreto Municipal n° 087/2015, e MEDIANTE APRESENTAÇÃO DAS CERTIDÕES ABAIXO RELACIONADAS**, JUNTAMENTE COM AS NOTAS FISCAIS:**

a) Prova de regularidade com a Fazenda Federal ou Certidão Conjunta prevista na Portaria MF nº 358, de 05 de setembro de 2014; Prova de regularidade (certidão) com a Seguridade Social - INSS ou Certidão Conjunta prevista na Portaria MF nº 358, de 05 de setembro de 2014; Prova de regularidade (certidão) com o FGTS (Fundo de Garantia do Tempo de Serviço); Prova de regularidade com a Fazenda Estadual sede da licitante; Prova de regularidade com a Fazenda do Município sede da licitante; Prova de regularidade com a Fazenda do Município de Presidente Kennedy e Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei n° 5.452, de 1° de maio de 1943, em atendimento a Lei 12.440/11, através de certidões expedidas pelos órgãos competentes, que estejam dentro do prazo de validade expresso na própria certidão.

b) A cada solicitação de pagamento a Contratada deverá comprovar que mantém todas as condições de habilitação e qualificações exigidas, juntando à solicitação de pagamento toda documentação apresentada no momento da licitação.

CLÁUSULA SEXTA - Dos Recursos Orçamentários

6.1. As despesas decorrentes da execução deste contrato correrão à conta dotação orçamentária: **Secretaria Municipal de Administração**. Projeto/Atividade: **3.107** - Aquisição de Link, implantação e Manutenção da logística digital no município. Elemento de Despesa: 33903900000 - Outros serviços de terceiros - Pessoa Jurídica. Fonte de Recurso: 15300000000 - Transferência da União referente Royalties do Petróleo

CLÁUSULA SETIMA - Das Penalidades e Sanções

7.1 - A empresa contratada deverá observar rigorosamente as condições estabelecidas para prestação dos serviços adjudicados, sujeitando-se às penalidades constantes no artigo 86 e 87 da Lei 8.666/93 e suas alterações e do art. 7º da Lei 10.520/02, a saber:

7.1.1 - Suspensão do direito de licitar pelo período de até 02 (dois) anos, em caso de manter-se inerte por período superior a 15 (quinze) dias do ato que deva praticar;

7.1.2 - Multa pelo atraso em prazo estipulado após a adjudicação do objeto, calculada pela fórmula:

M = 0,5 x C x D
onde:
M = valor da multa
C = valor da obrigação
D = número de dias em atraso

7.1.3 - Pelo não fornecimento e prestação dos serviços contratados, multa de 2 % (dois por cento) do valor do Contrato, e nessa hipótese, poderá ser revogada a licitação ou convocar os licitantes remanescentes, na ordem de classificação, para fazer o fornecimento e prestação de serviços, nas mesmas condições propostas pelo primeiro classificado;

7.1.4 - Declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos da punição, ou até que seja promovida a reabilitação perante a autoridade que aplicou a penalidade, o que será concedido sempre que a CONTRATADA ressarcir o Município pelos prejuízos resultantes e depois de decorrido o prazo da sanção aplicada;

7.1.4.1- A sanção de "declaração de inidoneidade" é de competência do Secretário da Pasta, facultada a defesa do interessado no respectivo processo, no prazo de 10 (dez) dias da abertura de vista ao processo, podendo a reabilitação ser requerida após 02 (dois) anos de sua aplicação.

7.2 - Juntamente com a aplicação das penalidades e sanções prevista nos itens acima, deverá ser observado pela Administração o disposto na INSTRUÇÃO NORMATIVA DO SISTEMA DE COMPRAS LICITAÇÕES E CONTRATOS - SCL Nº 007/2016, aprovada pelo Decreto Municipal Nº 58/2016.

CLÁUSULA OITAVA - DA RESCISÃO

8.1 - A inexecução total ou parcial do contrato enseja a sua rescisão, com as consequências contratuais e as previstas em lei, bem como a aplicação das multas e penalidades previstas neste instrumento.

8.2- **Constituem motivo para rescisão do contrato:**

I - o não cumprimento de cláusulas contratuais, especificações, projetos ou prazos;

II - o cumprimento irregular de cláusulas contratuais, especificações, projetos ou prazos;

III- a lentidão do seu cumprimento, levando a administração a comprovar a impossibilidade da conclusão do fornecimento nos prazos estipulados;

IV- o atraso injustificado no fornecimento do objeto da prestação dos serviços;

V - a paralisação da prestação dos serviços sem justa causa e prévia comunicação à Administração;

VI- a sub-contratação total do seu objeto, a associação da CONTRATADA com outrem, a cessão ou transferência, total ou parcial, bem como a fusão, cisão ou incorporação;

VII- o desatendimento das determinações regulares da autoridade designada para acompanhar e fiscalizar a sua execução, assim como as de seus superiores;

VIII- o cometimento reiterado de faltas na sua execução, anotadas na forma do § 1º do art. 67 da Lei nº 8.666/93;

IX - a decretação de falência, ou a instauração de insolvência civil;

X - a dissolução da sociedade;

XI - a alteração social ou a modificação da finalidade ou da estrutura da empresa, que, a juízo da CONTRATANTE, prejudique a execução do contrato;

XII- razões de interesse público de alta relevância e amplo conhecimento, justificadas e determinadas pela máxima autoridade da esfera administrativa a que está subordinada a CONTRATANTE e exaradas no processo administrativo a que se refere o contrato;

XIII - a ocorrência de casos fortuitos ou de força maior, regularmente comprovada, impeditiva da execução do contrato;

XIV - o atraso superior a 90 (noventa) dias dos pagamentos devidos pela Administração decorrentes dos serviços já prestados, salvo em caso de calamidade pública, grave perturbação da ordem interna ou guerra, assegurado à CONTRATADA o direito de optar pela suspensão do cumprimento de suas obrigações até que seja normalizada a situação;

XV - a supressão, por parte da Administração, dos serviços, acarretando modificação do valor inicial do contrato além do limite permitido no § 1º do art. 65 da Lei nº 8.666/93.

8.2.1. A decisão da autoridade competente, relativa à rescisão do contrato, deverá ser precedida de justificativa fundada, assegurado o contraditório e a ampla defesa.

8.3. **- A rescisão do contrato poderá ser:**

I- determinada por ato unilateral e escrito da CONTRATANTE, nos casos enumerados nos incisos **I** à **XIII** do item 8.2;

II - amigável, por acordo entre as partes e reduzida a termo no processo da licitação, desde que haja conveniência para a administração;

III - judicial, nos termos da legislação.

8.3.1. A rescisão administrativa ou amigável deverá ser precedida de autorização escrita e fundamentada do Secretário da Pasta.

CLÁUSULA NONA - Da Responsabilidade das Partes

9.1 - Constituem obrigações da CONTRATANTE:

9.1.1 - Efetuar a CONTRATADA o pagamento de preço ajustado na **Cláusula Quarta** e nos termos estabelecidos na Cláusula Quinta.

9.1.2 - Designar servidor(es) responsável(eis) pelo acompanhamento e fiscalização do objeto deste Contrato.

9.1.3 - Cumprir as cláusulas de responsabilidade e obrigações contidas no Termo de Referência.

9.2 - Constituem obrigações da CONTRATADA:

9.2.1 - Executar o objeto contrato nos termos do **TERMO DE REFERÊNCIA** anexo ao **Edital** e Proposta da CONTRATADA,

assim como de acordo com o previsto neste Contrato, por intermédio exclusivo de seus empregados.

9.2.2 - Pagar todos os encargos trabalhistas, previdenciários, fiscais e comerciais resultantes da execução deste instrumento, como estabelece no art. 71 da Lei nº 8.666/93, bem como seguros e quaisquer outros não mencionados, bem como pagamento de todo e qualquer tributo que seja devido em decorrência direta ou indireta do contrato, isentando a CONTRATANTE de qualquer responsabilidade.

9.2.3 - Utilizar, no fornecimento dos objetos contratados, pessoal que atenda aos requisitos de qualificação necessária ao exercício das atividades que lhe for confiada;

9.2.4 - Registrar as ocorrências havidas durante a execução deste Contrato, de tudo dando ciência à CONTRATANTE, respondendo integralmente por sua omissão.

9.2.5 - Apresentar documento fiscal hábil, sem emendas ou rasuras.

9.2.6 - Assumir inteira responsabilidade civil, administrativa e penal por quaisquer danos e prejuízos, materiais ou pessoais causados pela CONTRATADA, seus empregados, ou prepostos à CONTRATANTE, ou a terceiros.

9.2.7 - Manter, durante a vigência do Contrato, todas as condições de habilitação e qualificação exigidas nesta licitação.

9.2.8 - **Não ceder ou subcontratar, parcial ou totalmente os serviços ou produtos objeto deste Contrato.**

9.2.9 - Cumprir as cláusulas de responsabilidade e obrigações contidas no Termo de Referência.

CLÁUSULA DÉCIMA - Dos Documentos exigidos para fins de Assinatura do Contrato

10.1 - **A LICITANTE deverá apresentar** declaração do Fabricante informando que a LICITANTE está autorizada a comercializar, instalar, configurar e prestar suporte técnico na solução ofertada;

10.2 - **A LICITANTE deverá apresentar** declaração do Fabricante informando que seu produto atende a todas as características e funcionalidades exigidas e contidas neste edital, devidamente acompanhada da indicação do (s) Código (s) e Nome (s) dos seus Softwares propostos para fornecimento do objeto deste edital;

10.3 - A LICITANTE deverá apresentar declaração que possuir técnicos certificados pelo Fabricante da solução para comprovar qualificação para execução do serviço.

10.4 - A LICITANTE deverá emitir declaração que cumpre todos os requisitos técnicos do edital se responsabilizando por isso, sendo que os requisitos técnicos serão validados pela equipe técnica de homologação.

CLÁUSULA DÉCIMA PRIMEIRA - Do Treinamento

11.1 - Deverá ser fornecido treinamento para a solução de firewall adquirida (hardware ou software) para a equipe do cliente;

11.2 - Carga Horária mínima de 30 horas;

11.3 - O instrutor deverá ser certificado pela fabricante dos produtos para realizar os treinamentos, este deverá ser comprovado mediante apresentação de certificado expedido pela fabricante da solução de segurança da informação;

11.4 - O material a ser fornecido no treinamento deverá ser o material certificado pelo próprio fabricante, não serão aceitas cópias de apostilas;

11.5 - Toda a infraestrutura, os custos de material (apostilas, manuais, etc.), alimentação (coffee break), instrutor (deslocamento, hospedagem e vencimentos) ficará a cargo da CONTRATADA;

11.6 - O treinamento deverá conter em seu conteúdo questões práticas e teóricas sobre o funcionamento e os recursos da solução proposta;

11.7 - Deverá ser fornecido um 01 lanche (coffee break) para cada 4 horas de treinamento suficiente para todos os alunos;

11.8 - Deve ser incluído, caso exista, módulos básicos e avançados de modo a cobrir todas as funcionalidades da solução ofertada;

11.9 - Este treinamento poderá ser realizado em ambiente externo ao da CONTRATANTE, inclusive com os recursos para laboratórios (handson) salvo em caso de necessidade e acordo entre CONTRATADA e CONTRATANTE;

11.10 - Os cursos deverão ser realizados em horários e data a serem acordados pela CONTRATADA e CONTRATANTE;

11.11 - A CONTRATADA deverá ofertar as instalações na localidade da CONTRATANTE para a realização dos treinamentos com os requisitos mínimos de infraestrutura de sala de treinamento;

CLÁUSULA DÉCIMA SEGUNDA - Da Garantia

12.1 - Toda solução deverá ser fornecida com suas respectivas licenças de funcionamento em sua capacidade total, com garantia de 03 (três) anos;

12.2 - Os equipamentos descritos nas Especificações Técnicas, deverão ter garantia mínima de 36 meses, contados a partir do aceite da fiscalização do contrato;

12.3 - Durante o período de garantia, a(s) contratada(s) deverá(ão) disponibilizar um número de contato telefônico da cidade de Vitória (prefixo 027) ou DDG (0800) para abertura de chamado técnico, que deverá ser identificado por um número, por uma data e por uma hora, para que o mesmo possa ser devidamente acompanhado;

12.4 - A contratada fornecerá, na data de assinatura do contrato, endereço eletrônico e número de fax para eventual contato que se faça necessário, no caso de indisponibilidade do acesso telefônico;

12.5 - A impossibilidade de recebimento da abertura de chamado através de tentativa nos canais de atendimento informados não exime o fornecedor do prazo de manutenção;

12.6 - A garantia será prestada na modalidade *on site* e deverá incluir os serviços de manutenção para resolução de problemas de hardware ou software, com substituição de peças ou equipamentos defeituosos, sem qualquer limitação quanto ao quantitativo das mesmas, por outros originais e em estado de novo, compatíveis com as características técnicas especificadas ou superiores, sem quaisquer ônus adicionais para a PMPK;

12.7 - Durante o período da garantia do equipamento, a(s) CONTRATADA(s) deverá(ão) prover suporte telefônico para todo problema de hardware, software e configuração dos equipamentos

12.8 - O início do atendimento deverá ser realizado em até 24 (vinte e quatro) horas após a abertura do chamado

12.9 - As despesas relativas ao transporte de equipamentos, incluindo serviços de manutenção ou substituição, deverão correr por conta da CONTRATADA;

12.10 - A fiscalização da PMPK será responsável pelo "ateste" na(s) Nota(s) Fiscal(is), acompanhamento da entregas dos equipamentos e assistência técnica na garantia;

12.11 - A(s) CONTRATADA(s) deverá(ão) comunicar por escrito à fiscalização contratual, imediatamente, a impossibilidade de execução de qualquer obrigação contratual, para a adoção das providências cabíveis;

12.13 - A falta de peças e/ou equipamentos não poderá ser alegada como motivo de força maior, e não exime a(s) CONTRATADA(s) das penalidades a que está(ão) sujeita(s) pelo não cumprimento dos prazos estabelecidos;

12.14 - A(s) CONTRATADA(s) deverá(ão) fornecer correções automáticas das versões de software / firmware durante o período de garantia, caso seja detectado algum problema;

12.15 - A(s) CONTRATADA(s) deverá(ão) garantir a total compatibilidade da solução proposta com novas implementações tecnológicas que vierem a ser desenvolvidas pelo fabricante do equipamento fornecido, visando assegurar a evolução e continuidade da base instalada;

12.16 - Os empregados da CONTRATADA deverão trajar uniforme com logotipo da empresa e crachá de identificação, enquanto permanecerem nas dependências da CONTRATANTE;

12.17 - A(s) CONTRATADA(s) assumirá(ão) inteira responsabilidade pela execução dos eventuais serviço no prazo de garantia, correndo por sua própria conta quaisquer ônus, encargos sociais, trabalhistas, previdenciários, tributos, taxas, licenças e férias, concernentes à contratação, inclusive seguros contra acidentes de trabalho, bem como o de indenizar todo e qualquer dano e prejuízo pessoal ou material que possa advir, direta ou indiretamente, no exercício de suas atividades;

12.18 - Os serviços deverão ser executados com observância das especificações técnicas e regulamentação aplicável ao caso, com esmero e correção, refazendo tudo quanto for impugnado pela fiscalização, se necessário;

12.20 - As despesas relativas aos eventuais deslocamentos do equipamento ou insumos deverão ocorrer integralmente por conta da(s) CONTRATADA(s), sem quaisquer ônus adicionais para o CONTRATANTE, durante todo o período de garantia;

12.21 - Deverão ser obedecidas as normas de segurança e medicina do trabalho para esse tipo de atividade, ficando

por conta da(s) CONTRATADA(s) o fornecimento, antes do início da execução dos serviços, dos Equipamentos de Proteção Individual - EPI, se necessário;

12.22 - Indicar, na data de assinatura do contrato, nome e telefone de funcionário que atuará como preposto, conforme preceitua o art. 68 da Lei 8666/93.

12.23 - Observações:

12.24 - Os prazos deste item poderão ser prorrogados mediante justificativa escrita da(s) CONTRATADA(s), submetida à apreciação do fiscal do CONTRATANTE.

CLÁUSULA DÉCIMA TERCEIRA - Do Acompanhamento e da Fiscalização

13.1- A execução deste Contrato será acompanhada por servidor previamente designado pela Administração, nos termos do art. 67 da Lei nº 8.666/93, que deverá atestar a realização dos serviços contratados, para cumprimento das normas estabelecidas nos art. 62 e 63 da Lei nº 4.320/64.

CLÁUSULA DÉCIMA QUARTA - Da Legislação Aplicável

14.1. - Aplica-se à execução deste Termo Contratual, em especial aos casos omissos, a Lei nº 8.666/93 e outras legislações correlatas.

CLÁUSULA DÉCIMA QUINTA - Dos Aditamentos

15.1. - O presente Contrato poderá ser aditado, nas hipóteses previstas em lei.

CLÁUSULA DÉCIMA SEXTA - Da Publicação

16.1. - O presente Contrato será publicado, em resumo, nono Diário Oficial dos Municípios do Espirito Santo, dando-se cumprimento ao disposto no art. 61, parágrafo único da Lei nº 8.666/93, correndo a despesa por conta da CONTRATANTE.

CLÁUSULA DÉCIMA SÉTIMA - Do Foro

17.1. - Fica eleito o foro da cidade de Presidente Kennedy/ES, para dirimir quaisquer dúvidas oriundas deste Contrato e que não possam ser resolvidas por meios administrativos, com renúncia a qualquer outro, por mais privilegiado que seja.

17.2. -E estando assim, justos e contratados, assinam o presente contrato em 03 (três) vias, de igual teor e forma, para que produza seus efeitos jurídicos e legais.

Presidente Kennedy-ES, _____de_____de_____.

_____

Secretaria Municipal de

_____

Contratada