ORIGEM DA LICITAÇÃO	**SECRETARIA MUNICIPAL DO PLANEJAMENTO, ORÇAMENTO E GESTÃO – SEPOG**
MODALIDADE:	**PREGÃO ELETRÔNICO Nº 134/2017**
PROCESSO N°:	**P661335/2017**
OBJETO:	**CONSTITUI OBJETO DA PRESENTE LICITAÇÃO A CONTRATAÇÃO DE EMPRESA ESPECIALIZADA NO FORNECIMENTO DE SOLUÇÃO INTEGRADA DE SEGURANÇA DE PERÍMETRO (FIREWALL), QUE POSSIBILITE A VISIBILIDADE E CONTROLE DE TRÁFEGO, FILTRAGEM DE CONTEÚDO WEB, PREVENÇÃO CONTRA AMEAÇAS DE REDES MODERNAS, FILTRO DE DADOS, VPN E CONTROLE GRANULAR DE BANDA DE REDE, COMPREENDENDO FORNECIMENTO DE EQUIPAMENTOS E SOFTWARES INTEGRADOS, *APPLIANCE*, LICENCIAMENTO E GARANTIA DE ATUALIZAÇÃO PARA ATENDER AS NECESSIDADES DA PREFEITURA MUNICIPAL DE FORTALEZA, DE ACORDO COM AS ESPECIFICAÇÕES E QUANTITATIVOS CONTIDOS NO ANEXO A – TERMO DE REFERÊNCIA DESTE EDITAL, PARA O PERÍODO DE 12 MESES.**

ÍNDICE DO EDITAL E SEUS ANEXOS

ASSUNTO	
1. DO TIPO.....	03
2. DA MODALIDADE	03
3. DA FORMA DE FORNECIMENTO	04
4. DA BASE LEGAL	04
5. DO OBJETO	04
6. DA RELAÇÃO DE LOTES DO PREGÃO 134/2017	04
7. DO ACESSO AO EDITAL E DO LOCAL DE REALIZAÇÃO	04
8. DAS DATAS E HORÁRIOS DO CERTAME	05

9. DO ENDEREÇAMENTO PARA ENTREGA DE DOCUMENTAÇÃO	05
10. DOS RECURSOS ORÇAMENTÁRIOS	05
11. DAS CONDIÇÕES DE PARTICIPAÇÃO	05
12. DA FORMA DE APRESENTAÇÃO DA PROPOSTA ELETRÔNICA	06
13. DA ABERTURA E ACEITABILIDADE DAS PROPOSTAS.....	07
14. DA ETAPA DE LANCES.....	08
15. DO LICITANTE ARREMATANTE.....	09
16. DA PROPOSTA DE PREÇOS ESCRITA.....	10
17. DA HABILITAÇÃO	11
18. OUTRAS DISPOSIÇÕES	16
19. DOS BENEFÍCIOS PARA ME E EPPS.....	16
20. DOS CRITERIOS DE JULGAMENTO	16
21. SERÃO DESCLASSIFICADAS AS PROPOSTAS DE PREÇOS.....	17
22. DOS PEDIDOS DE ESCLARECIMENTOS E IMPUGNAÇÕES.....	18
23. DOS RECURSOS ADMINISTRATIVOS.....	18
24. DA ADJUDICAÇÃO, DA HOMOLOGAÇÃO	19
25. DAS SANÇÕES ADMINISTRATIVAS.....	19
26. DA CONTRATAÇÃO	20
27. DA GARANTIA CONTRATUAL	21
28. DAS DISPOSIÇÕES GERAIS.....	21
29. DOS ANEXOS.....	22
ANEXO A – TERMO DE REFERÊNCIA.....	24
ANEXO B - MODELO DA PROPOSTA DE PREÇOS.....	51
ANEXO C – MODELO MERAMENTE SUGESTIVO DE DECLARAÇÃO DE MICROEMPRESA, EMPRESA DE PEQUENO PORTE OU COOPERATIVA (***entregar junto com a proposta de preços escrita***)	53

ANEXO D – MODELO DE **DECLARAÇÃO DE CONTRATOS FIRMADOS COM A INICIATIVA PRIVADA E ADMINISTRAÇÃO PÚBLICA**.....	54
ANEXO E – MINUTA DO CONTRATO	55
ANEXO F – DECLARAÇÃO RELATIVA AO TRABALHO DE EMPREGADO MENOR.....	80
ANEXO G – MODELO DE ORDEM DE SERVIÇO	81
ANEXO H - ANÁLISE DAS AMOSTRAS	82
ANEXO I – GLOSSÁRIO	84

PROCESSO Nº. P661335/2017

PREGÃO ELETRÔNICO N° 134/2017

CONSTITUI OBJETO DA PRESENTE LICITAÇÃO A CONTRATAÇÃO DE EMPRESA ESPECIALIZADA NO FORNECIMENTO DE SOLUÇÃO INTEGRADA DE SEGURANÇA DE PERÍMETRO (FIREWALL), QUE POSSIBILITE A VISIBILIDADE E CONTROLE DE TRÁFEGO, FILTRAGEM DE CONTEÚDO WEB, PREVENÇÃO CONTRA AMEAÇAS DE REDES MODERNAS, FILTRO DE DADOS, VPN E CONTROLE GRANULAR DE BANDA DE REDE, COMPREENDENDO FORNECIMENTO DE EQUIPAMENTOS E SOFTWARES INTEGRADOS, *APPLIANCE*, LICENCIAMENTO E GARANTIA DE ATUALIZAÇÃO PARA ATENDER AS NECESSIDADES DA PREFEITURA MUNICIPAL DE FORTALEZA, DE ACORDO COM AS ESPECIFICAÇÕES E QUANTITATIVOS CONTIDOS NO ANEXO A – TERMO DE REFERÊNCIA DESTE EDITAL, PARA O PERÍODO DE 12 MESES.

O titular da origem desta licitação torna público, para conhecimento dos interessados, que o(a) Pregoeiro(a) regulamentado(a) através do Decreto Municipal nº 13.512, de 30 de dezembro de 2014 e nomeado(a) por Ato juntado ao processo administrativo de que trata esta licitação, devidamente publicados no Diário Oficial do Município, assessorado(a) pela equipe de apoio também designada formalmente por ato publicado no DOM e juntado ao processo, receberá e abrirá eletronicamente até horas, data e local abaixo indicados as **PROPOSTAS DE PREÇOS** e em momento seguinte **DOCUMENTOS DE HABILITAÇÃO** referentes à licitação objeto deste instrumento para a escolha da proposta mais vantajosa, objetivando a contratação objeto desta licitação, observadas as normas e condições do presente Edital e as disposições contidas na Lei nº 10.520 de 17 de julho de 2002, na Lei n° 8.666/93 publicada no Diário Oficial da União de 22/06/93, e suas alterações posteriores, e no Decreto Municipal nº 11.251, de 10 de setembro de 2002.

1. **DO TIPO:** MENOR PREÇO.

2. **DA MODALIDADE**: PREGÃO ELETRÔNICO

3. DA FORMA DE FORNECIMENTO: INTEGRAL.

4. DA BASE LEGAL: Lei Federal nº 10.520, de 17 de julho 2002, Lei Complementar nº 123, de 14 de dezembro de 2006, Lei Complementar nº 147 de 07 de agosto de 2014, nos Decretos Municipais nºs 11.251 de 10 de setembro de 2002, nº 13.512 de 30 de dezembro de 2014, n° 13.735 de 18 de janeiro de 2016 e subsidiariamente a Lei Federal nº. 8.666, de 21 de junho de 1993, com suas alterações e do disposto no presente edital e seus anexos.

5. DO OBJETO:

CONSTITUI OBJETO DA PRESENTE LICITAÇÃO A CONTRATAÇÃO DE EMPRESA ESPECIALIZADA NO FORNECIMENTO DE SOLUÇÃO INTEGRADA DE SEGURANÇA DE PERÍMETRO (FIREWALL), QUE POSSIBILITE A VISIBILIDADE E CONTROLE DE TRÁFEGO, FILTRAGEM DE CONTEÚDO WEB, PREVENÇÃO CONTRA AMEAÇAS DE REDES MODERNAS, FILTRO DE DADOS, VPN E CONTROLE GRANULAR DE BANDA DE REDE, COMPREENDENDO FORNECIMENTO DE EQUIPAMENTOS E SOFTWARES INTEGRADOS, *APPLIANCE*, LICENCIAMENTO E GARANTIA DE ATUALIZAÇÃO PARA ATENDER AS NECESSIDADES DA PREFEITURA MUNICIPAL DE FORTALEZA, DE ACORDO COM AS ESPECIFICAÇÕES E QUANTITATIVOS CONTIDOS NO ANEXO A – TERMO DE REFERÊNCIA DESTE EDITAL, PARA O PERÍODO DE 12 MESES.

6. DA RELAÇÃO DE LOTE DO PREGÃO 134/2017:

6.1. Sob pena de desclassificação, os licitantes deverão apresentar suas propostas, obedecendo as especificações técnicas, bem como requisitos mínimos exigidos no Anexo A – termo de referência deste edital.

LOTE ÚNICO		
ITEM	**DESCRIÇÃO**	**QUANTIDADE**
01	Solução de alta disponibilidade de *Next Generation Firewall*, com garantia de funcionamento, atualização de assinaturas de proteção e suporte técnico local e remota, 24x7, pelo prazo de 36 meses (trinta e seis) meses, incluindo serviços de instalação.	01

7. DO ACESSO AO EDITAL E DO LOCAL DE REALIZAÇÃO:

7.1. O edital está disponível gratuitamente nos *sítios* compras.fortaleza.ce.gov.br e www.licitacoes-e.com.br.

7.2. O certame será realizado por meio do sistema do Banco do Brasil, no endereço eletrônico www.licitacoes-e.com.br.

8. DAS DATAS E HORÁRIOS DO CERTAME:

8.1. **INÍCIO DO ACOLHIMENTO DAS PROPOSTAS**: 12/06/2017

8.2. **DATA DE ABERTURA DAS PROPOSTAS**: 26/06/2017, às 09h00min.

8.3. **INÍCIO DA SESSÃO DE DISPUTA DE PREÇOS**: 26/06/2017, às 14h00min.

8.4. **REFERÊNCIA DE TEMPO**: Para todas as referências de tempo utilizadas pelo sistema será observado o horário de **Brasília/DF.**

8.5. Na hipótese de não haver expediente ou ocorrendo qualquer fato superveniente que impeça a realização do certame na data prevista, a sessão será remarcada, para no mínimo 48h (quarenta e oito horas) a contar da respectiva data.

9. DO ENDEREÇAMENTO PARA A ENTREGA DE DOCUMENTAÇÃO:

9.1. A documentação deverá ser entregue no endereço sito à Rua do Rosário, 77, Centro – Ed. Comte. Vital Rolim – Sobreloja e Terraço, Fortaleza-Ce, CEP. 60055-090.

9.2. A documentação será apresentada em envelope lacrado contendo no anverso o nome do pregoeiro, número do pregão e o nome do órgão.

10. DOS RECURSOS ORÇAMENTÁRIOS:

10.1. As despesas decorrentes desta licitação correrão à conta das dotações consignadas abaixo:

Projeto Atividade: 04.126.0106.1062.0001, Elementos de Despesa: 44.90.39 e 44.9052, Fontes de Recurso: 30101 e 33101, do orçamento da Secretaria Municipal do Planejamento, Orçamento e Gestão – SEPOG.

11. DAS CONDIÇÕES DE PARTICIPAÇÃO

11.1. Os interessados em participar deste certame deverão estar credenciados junto ao sistema do Banco do Brasil S.A.

11.1.1. As regras para credenciamento estarão disponíveis no sítio constante no **subitem 7.2** deste edital.

11.2. Será garantido aos licitantes enquadrados como microempresas e empresas de pequeno porte e as cooperativas que se enquadrem nos termos do art. 34, da Lei Federal n° 11.488/2007, como

critério de desempate, preferência de contratação, o previsto na Lei Complementar n° 123/2006, em seu Capítulo V – DO ACESSO AOS MERCADOS / Das Aquisições Públicas e Lei Complementar nº 147 de 07 de agosto de 2014, bem como Lei Municipal 10.350 de 28/05/2015 em seu capítulo IV, Subseção III – Do direito de preferência e outros incentivos), e Art. 33 do Decreto Municipal n° 13.735 de 18 de janeiro de 2016.

11.3. Tratando-se de microempresas e empresas de pequeno porte deverão declarar no Sistema do Banco do Brasil o exercício da preferência prevista na Lei Complementar n° 123/2006.

11.4. A participação implica a aceitação integral dos termos deste edital.

11.5. É vedada a participação de pessoa física e de pessoa jurídica nos seguintes casos:

11.5.1. Sob a forma de consórcio, qualquer que seja sua constituição.

11.5.2. Que tenham em comum um ou mais sócios cotistas e/ou prepostos com procuração.

11.5.3. Que estejam em estado de insolvência civil, sob processo de falência, concordata, recuperação judicial ou extrajudicial, dissolução, fusão, cisão, incorporação e liquidação.

11.5.4. Impedidas de licitar e contratar com a Administração.

11.5.5. Suspensas temporariamente de participar de licitação

11.5.6. Declaradas inidôneas pela Administração Pública, enquanto perdurarem os motivos determinantes desta condição.

11.5.7. Servidor público ou empresas cujos dirigentes, gerentes, sócios ou componentes de seu quadro técnico sejam funcionários ou empregados públicos da Administração Pública Municipal Direta ou Indireta.

11.5.8. Estrangeiras não autorizadas a comercializar no país.

12. DA FORMA DE APRESENTAÇÃO DA PROPOSTA ELETRÔNICA

12.1. Os licitantes deverão enviar suas propostas até a data e hora designadas para a abertura das mesmas, consignando o preço global do lote incluído todos os custos diretos e indiretos, de acordo com o especificado neste edital.

12.2. Nos preços deverão estar inclusos todos os custos diretos e indiretos, lucro, encargos trabalhistas e despesas com seguros, frete, mão-de-obra e outras necessárias ao cumprimento integral do objeto deste Pregão e excluídos da composição dos preços ofertados o imposto de renda pessoa jurídica (IRPJ) e a contribuição social sobre o lucro líquido (CSLL).

12.3. Os licitantes enquadrados como ME ou EPP deverão declarar que cumprem plenamente os requisitos de habilitação, bem como, caso exista, indicar no ato do envio das propostas eletrônicas a existência de restrição da documentação exigida para fins de habilitação, referentes à regularidade fiscal, observado o subitem 12.7 deste edital.

12.4. No campo “Informações Adicionais” deverá constar necessariamente o seguinte:

a) Indicação do lote cotado e especificação do objeto da licitação de acordo com o disposto no ANEXO A deste edital, devendo ser indicada a marca e/ou fabricante do produto;
b) Preço global do lote cotado em algarismos;
c) Prazo de validade da proposta que não poderá ser inferior a 90 (noventa) dias.

12.5. O licitante deverá informar a condição de microempresa (ME) ou empresa de pequeno porte (EPP) que faz jus ao tratamento diferenciado da Lei Complementar n° 123, de 2006, ou cooperativa de que trata o artigo 34 da Lei nº 11.488, de 2007, no ato do envio da proposta.

12.6. Os licitantes poderão retirar ou substituir as propostas por eles apresentadas, até o término do prazo para recebimento.

12.7. Será vedada a identificação do licitante.

13. DA ABERTURA E ACEITABILIDADE DAS PROPOSTAS

13.1. Abertas as propostas, o pregoeiro fará as devidas verificações, avaliando a aceitabilidade das mesmas. Caso ocorra alguma desclassificação, deverá ser fundamentada e registrada no sistema.

13.2. Os preços deverão ser expressos em reais, com até 2 (duas) casas decimais em seus valores globais e unitários, inclusive em propostas de adequação, quando for o caso.

13.3. O sistema ordenará automaticamente as propostas classificadas pelo pregoeiro e somente estas participarão da etapa de lances.

13.4. **Na elaboração da proposta, o preço cotado poderá ultrapassar o limite máximo discriminado no mapa de preços, presente nos autos do processo em epígrafe; entretanto, na fase de lances, o lance final deverá atingir preço igual ou inferior ao limite máximo constante daquele mapa de preços. Caso não seja realizada a fase de lances, o licitante que cotou na proposta o menor preço deverá reduzi-lo a um valor igual ou inferior ao limite máximo do referido mapa de preços.**

14. DA ETAPA DE LANCES

14.1. O pregoeiro dará início à etapa competitiva no horário previsto no **subitem 8.3**, quando, então, os licitantes poderão encaminhar lances, que deverão ser apresentados exclusivamente por meio do sistema eletrônico, sendo o licitante imediatamente informado do seu recebimento e respectivo horário de registro e valor.

14.2. Para efeito de lances, será considerado o **valor global do lote**.

14.2.1. Na fase de lances, o lance final deverá atingir preço igual ou inferior ao limite máximo constante daquele mapa de preços. Caso não seja realizada a fase de lances, o licitante que cotou na proposta o menor preço deverá reduzi-lo a um valor igual ou inferior ao limite máximo do referido mapa de preços.

14.2.2. Os licitantes poderão ofertar lances sucessivos, desde que inferiores ao seu último lance registrado no sistema, ainda que este seja maior que o menor lance já ofertado por outro licitante.

14.2.3. Em caso de dois ou mais lances de igual valor, prevalece aquele que for recebido e registrado em primeiro lugar.

14.3. Durante a sessão pública de disputa, os licitantes serão informados, em tempo real, do valor do menor lance registrado. O sistema não identificará o autor dos lances ao pregoeiro nem aos demais participantes.

14.4. No caso de desconexão entre o pregoeiro e o sistema no decorrer da etapa competitiva, o sistema poderá permanecer acessível à recepção dos lances, retornando o pregoeiro, quando possível, sem prejuízos dos atos realizados.

14.4.1. Quando a desconexão persistir por tempo superior a 10 (dez) minutos, a sessão será suspensa, sendo reiniciada somente após comunicação expressa do pregoeiro aos participantes, através de mensagem no sistema, divulgando data e hora da reabertura da sessão. Caberá ao licitante a responsabilidade por qualquer ônus decorrente da perda de negócio diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão.

14.5. A etapa inicial de lances será encerrada pelo pregoeiro, seguida do tempo randômico, que poderá ser de 1 (um) segundo a 30 (trinta) minutos, aleatoriamente determinado pelo sistema eletrônico.

14.6. Transcorrido o tempo randômico, o sistema detectará a existência de situação de empate ficto. Em cumprimento ao que determina a Lei Complementar nº 123/2006, a microempresa, a empresa de pequeno porte e a cooperativa que se enquadre nos termos do art. 34, da Lei Federal nº 11.488/2007 e que ofertou lance de até 5% (cinco por cento) superior ao menor preço da arrematante que não se enquadre nessa situação de empate, será convocada pelo pregoeiro, na sala de disputa, para, no prazo de 5 (cinco) minutos, utilizando-se do direito de preferência, ofertar novo lance inferior ao melhor lance registrado, sob pena de preclusão.

14.6.1. Caso a ME ou EPP melhor classificada seja de outro Estado da Federação e haja ME ou EPP inscrita no Cadastro Geral da Fazenda do Estado do Ceará em situação de empate descrito nos parágrafos primeiro e segundo do artigo 31 do Decreto Municipal 13.735, de 18 de janeiro de 2016, esta poderá apresentar proposta de preço inferior àquela apresentada por ME ou EPP de outro Estado da Federação, situação em que será adjudicado o objeto em seu favor, conforme estabelecido no art. 32, do Decreto Municipal nº 13.735/2016.

14.6.1.1. O disposto no subitem 14.6.1 não se aplica quando a melhor oferta válida tiver sido apresentada por microempresa ou empresa de pequeno porte.

14.6.2. Não havendo manifestação do licitante, o sistema verificará a existência de outro em situação de empate, realizando o chamado de forma automática. Não havendo outra situação de empate, o sistema emitirá mensagem, cabendo ao pregoeiro dar por encerrada a disputa do lote.

14.7. O sistema informará a proposta de menor preço ao encerrar a fase de disputa.

15. DO LICITANTE ARREMATANTE

15.1. O pregoeiro poderá negociar exclusivamente pelo sistema, em campo próprio, a fim de obter melhor preço.

15.2. A partir da sua convocação, o arrematante deverá encaminhar imediatamente, no prazo máximo de até 04 (quatro) horas através de FAX, para o número (85)3252.16.30 ou e-mail (licitacao@fortaleza.ce.gov.br) a **proposta de preços** e **a documentação de habilitação** e no prazo máximo de até 02(dois) dias úteis a contar do término da sessão virtual o arrematante deverá entregar, na Central de Licitações da Prefeitura de Fortaleza - CLFOR, no endereço constante no **subitem 9.1**, os documentos acima mencionados em original ou por cópia autenticada.

15.2.1. O arrematante que efetuar a **entrega da proposta de preços e da documentação de habilitação,** na sede da Central de Licitações da Prefeitura de Fortaleza- CLFOR, em conformidade com o subitem 15.2, no prazo de até 04 (quatro) horas, contadas de sua convocação, fica dispensado de encaminhar os mesmos documentos através de FAX ou e-mail.

15.2.2. O não cumprimento da entrega da documentação, dentro do prazo acima estabelecido, acarretará desclassificação/inabilitação, sendo convocado o licitante subsequente, e assim sucessivamente, observada a ordem de classificação.

16. DA PROPOSTA DE PREÇOS ESCRITA

16.1. A proposta deverá ser apresentada em via única original e numerada, com os preços ajustados ao menor lance, nos termos do Anexo B – Proposta de preços deste edital, com todas as folhas rubricadas, devendo a última folha vir assinada pelo representante legal do licitante citado na documentação de habilitação, em linguagem clara e concisa, sem emendas, rasuras ou entrelinhas, com as especificações técnicas, quantitativos, prazo de garantia, devendo ser indicada a marca e/ou fabricante do produto e demais informações relativas aos bens e serviço ofertados.

16.2. Prazo de validade não inferior a 90 (noventa) dias, contados a partir da data de sua emissão.

16.3. O licitante não poderá cotar proposta com quantitativo de item/lote inferior ao determinado no edital.

16.4. Na cotação do preço unitário, não será admitido o fracionamento do centavo.

16.5. Nos preços propostos já estarão incluídas as despesas referentes a frete, tributos e demais ônus atinentes à entrega do objeto.

16.6. No caso do licitante ser cooperativa que executará (entregará) o objeto da licitação através de empregados, a mesma gozará dos privilégios fiscais e previdenciários pertinente ao regime das cooperativas, devendo a proposta apresentar exequibilidade no aspecto tributário e sujeitar-se ao mesmo regime de qualquer outro agente econômico.

16.7. Após a apresentação da proposta não caberá desistência.

16.9. Deverá constar na proposta:

16.9.1. Deverá ser apresentada **Declaração da licitante enquadrada como Microempresa e Empresa de Pequeno Porte** acerca do exercício do direito de preferência previsto na Lei Complementar n° 123/2006, conforme modelo no Anexo C – DECLARAÇÃO DE MICROEMPRESA, EMPRESA DE PEQUENO PORTE OU COOPERATIVA.

16.9.2 Declaração da licitante constando o prazo de garantia dos produtos contra quaisquer defeitos de fabricação para todos os lotes cotados constantes no presente edital que não poderá ser inferior a 12 (doze) meses.

16.9.3 Declaração da licitante de que responde por todos os prejuízos, perdas e danos que venham a ocorrer referentes ao transporte e entrega dos produtos, caso venha a ser contratado.

16.10. APRESENTAÇÃO DE AMOSTRAS

16.10.1**.** Após a verificação da documentação original referente à proposta de preços escrita e à habilitação, o Pregoeiro deverá solicitar do arrematante, amostras dos produtos cotados objeto desta licitação para melhor avaliação, ficando o arrematante obrigado, sob pena de desclassificação, apresentar tais amostras no prazo definido no Anexo H – Análise da Amostra, deste Edital

16.10.2. Os prazos e demais procedimentos relativos à análise das amostras constam no Anexo H – Análise da Amostra.

16.10.3. Não será aceita a proposta da arrematante que tiver amostra rejeitada, que não enviar amostra, ou que não apresentá-la no prazo estabelecido.

16.10.4**.** Ao final da avaliação, o(s) equipamento(s) será(ão) devolvido(s) à arrematante.

16.10.5**.** Enquanto não expirado o prazo para entrega da amostra, a arrematante poderá substituir ou efetuar ajustes e modificações no produto apresentado.

16.10.6. A não conformidade de um ou mais itens em relação às especificações constantes deste Termo de Referência implica na recursa do lote inteiro, resultando na não aceitação da proposta.

17. DA HABILITAÇÃO

17.1. O licitante CADASTRADO deverá apresentar o Certificado de Registro Cadastral (CRC) emitido pela Central de Licitações da Prefeitura de Fortaleza - CLFOR, compatível com o ramo objeto licitado, e a regularidade trabalhista mediante prova de inexistência de débitos inadimplidos perante a justiça do trabalho, através da Certidão Negativa de Débitos Trabalhistas ou da Certidão Positiva de Débitos Trabalhistas com Efeitos Negativos, obrigando-se a declarar, sob as penalidades legais, a superveniência de fato impeditivo da habilitação, na forma do § 2°, do art. 32, da Lei Federal n° 8.666/1993.

17.1.1. O CRC não substituirá os documentos referentes à Qualificação Técnica.

17.1.2. O pregoeiro verificará a situação do licitante no Certificado de Registro Cadastral. Caso o mesmo esteja com algum documento vencido, deverá apresentá-lo juntamente com os documentos de habilitação, sob pena de inabilitação, salvo os documentos de Regularidades Fiscal e Trabalhista acessíveis para consultas em *sítios* oficiais que poderão ser consultados pelo pregoeiro.

17.2 OS DOCUMENTOS DE HABILITAÇÃO DEVERÃO SER APRESENTADOS DA SEGUINTE FORMA

17.2.1. Obrigatoriamente, da mesma sede, ou seja, se da matriz, todos da matriz, se de alguma filial, todos da mesma filial, com exceção dos documentos que são válidos tanto para matriz como para todas as filiais. O contrato será celebrado com a sede que apresentou a documentação referente à regularidade fiscal.

17.2.2. O documento obtido através de *sítios* oficiais, que esteja condicionado à aceitação via internet, terá sua autenticidade verificada pelo pregoeiro.

17.2.3. Caso haja documento redigido em idioma estrangeiro, o mesmo somente será considerado se acompanhado da versão em português, firmada por tradutor juramentado.

17.2.4. Dentro do prazo de validade. Na hipótese de o documento não constar expressamente o prazo de validade, este deverá ser acompanhado de declaração ou regulamentação do órgão emissor que disponha sobre sua validade. Na ausência de tal declaração ou regulamentação, o documento será considerado válido pelo prazo de 90 (noventa) dias, contados a partir da data de sua emissão, quando se tratar de documentos referentes à habilitação fiscal e econômico-financeira.

17.2.5. O licitante NÃO CADASTRADO no CRC junto à **Central de Licitações da Prefeitura de Fortaleza - CLFOR** deverá apresentar os documentos relacionados a seguir:

17.3 - **HABILITAÇÃO JURÍDICA**

17.3.1. **REGISTRO COMERCIAL**, no caso de empresa pessoa física, no registro público de empresa mercantil da Junta Comercial; devendo, no caso do licitante ser o sucursal, filial ou agência, apresentar o registro da Junta onde opera com averbação no registro da Junta onde tem sede a matriz.

17.3.2. **ATO CONSTITUTIVO, ESTATUTO OU CONTRATO SOCIAL CONSOLIDADO** em vigor devidamente registrado no registro público de empresa mercantil da Junta Comercial, em se tratando de sociedades empresárias e, no caso de sociedades por ações, acompanhado de documentos de eleição de seus administradores; devendo, no caso do licitante ser o sucursal, filial ou agência, apresentar o registro da Junta onde opera com averbação no registro da Junta onde tem sede a matriz.

17.3.3. **INSCRIÇÃO DO ATO CONSTITUTIVO**, no caso de sociedades simples - exceto cooperativas - no Cartório de Registro das Pessoas Jurídicas acompanhada de prova da diretoria em exercício; devendo, no caso do licitante ser o sucursal, filial ou agência, apresentar o registro no Cartório de Registro das Pessoas Jurídicas do Estado onde opera com averbação no Cartório onde tem sede a matriz.

17.3.4. **DECRETO DE AUTORIZAÇÃO**, em se tratando de empresa ou sociedade estrangeira em funcionamento no País, e **ATO DE REGISTRO DE AUTORIZAÇÃO PARA FUNCIONAMENTO** expedido pelo órgão competente, quando a atividade assim o exigir.

17.3.5. **REGISTRO NA ORGANIZAÇÃO DAS COOPERATIVAS BRASILEIRAS**, no caso de cooperativa, acompanhado dos seguintes documentos:

a) Ato constitutivo ou estatuto social, nos termos dos arts. 15 a 21 da lei 5.764/71;
b) Comprovação da composição dos órgãos de administração da cooperativa (diretoria e conselheiros), consoante art. 47 da lei 5.764/71;
c) Ata de fundação da cooperativa;
d) Ata de assembleia que aprovou o estatuto social;
e) Regimento interno com a Ata da assembleia que o aprovou;
f) Regimento dos fundos constituídos pelos cooperados com a Ata da assembleia que os aprovou;
g) Editais das 03 últimas assembleias gerais extraordinárias.

17.3.6. Alvará de Funcionamento da Empresa expedido por órgão público municipal da sede ou domicílio do licitante.

17.4. DA QUALIFICAÇÃO TÉCNICA

17.4.1. Comprovação de aptidão para o desempenho de atividade pertinente e compatível em características com o objeto da licitação, mediante apresentação de atestado(s) fornecido(s) por pessoa(s) jurídica(s) de direito público ou privado.

17.4.1.1. Os atestados deverão conter no mínimo o nome do contratado e da contratante, a identificação do objeto do contrato e os serviços executados (discriminação e quantidades);

17.4.1.2. Os atestados deverão possuir informações suficientes para qualificar o seu objeto, bem como possibilitar ao CONTRATANTE confirmar sua veracidade junto à instituição emissora do atestado;

17.4.1.3. Para verificar a autenticidade dos atestados apresentados, o CONTRATANTE poderá realizar diligências ou requerer os comprovantes fiscais da execução do objeto;

17.4.2. Licenciamento Ambiental da sede ou domicílio da licitante, perante o Órgão Ambiental competente, para exercer as atividades objeto deste edital, de acordo com a legislação vigente aplicável ou a isenção da licença ambiental que poderá ser comprovada por documento próprio conforme a legislação vigente ou alguma comprovação idônea da isenção.

17.5. DA QUALIFICAÇÃO ECONÔMICO-FINANCEIRA

17.5.1. Certidão negativa de falência, concordata, recuperação judicial ou extrajudicial, expedida por quem de competência na sede da pessoa jurídica ou certidão negativa de execução patrimonial expedida no domicílio da pessoa física.

17.5.1.1**.** No caso de cooperativa, a mesma está dispensada da apresentação da Certidão exigida no subitem acima item 17.5.1.

17.5.2. BALANÇO PATRIMONIAL e demonstrações contábeis do último exercício social, já exigíveis e apresentados na forma da lei, que comprovem a boa situação financeira do licitante, vedada a sua substituição por balancetes ou balanços provisórios, podendo ser atualizados por índices oficiais, quando encerrado há mais de 03 meses da data de apresentação da proposta.

17.5.3. COMPROVAÇÃO DA BOA SITUAÇÃO FINANCEIRA atestada por documento, assinado por profissional legalmente habilitado junto ao Conselho Regional de Contabilidade da sede ou filial do licitante, demonstrando que a empresa apresenta índice de Liquidez Geral (LG) maior ou igual a 1,0 (um vírgula zero), calculada conforme a fórmula abaixo:

$$LG = \frac{AC + ARLP}{PC + PELP} \geq 1,0$$

Onde:
LG – Liquidez Geral;
AC – Ativo Circulante;
ARLP – Ativo Realizável a Longo Prazo;
PC – Passivo Circulante;
PELP – Passivo Exigível a Longo Prazo;

17.5.4. No caso de sociedade por ações, o balanço deverá ser acompanhado da publicação em jornal oficial, em jornal de grande circulação e do registro na Junta Comercial.

17.5.5. No caso das demais sociedades empresárias, o balanço deverá ser acompanhado dos termos de abertura e de encerramento do Livro Diário - estes termos devidamente registrados na Junta Comercial - constando ainda, no balanço, o número do Livro Diário e das folhas nos quais se acha transcrito ou autenticada na junta comercial, devendo tanto o balanço quanto os termos ser assinados por contador registrado no Conselho Regional de Contabilidade e pelo titular ou representante legal da empresa.

17.5.6. No caso de empresa recém-constituída (há menos de 01 ano), deverá ser apresentado o balanço de abertura acompanhado dos termos de abertura e de encerramento devidamente registrados na Junta Comercial, constando no balanço o número do Livro e das folhas nos quais se acha transcrito ou autenticado na junta comercial, devendo ser assinado por contador registrado no Conselho Regional de Contabilidade e pelo titular ou representante legal da empresa.

17.5.7. No caso de sociedade simples e cooperativa - o balanço patrimonial deverá ser inscrito no Cartório de Registro Civil de Pessoas Jurídicas assinado por contador registrado no Conselho

Regional de Contabilidade e pelo titular ou representante legal da instituição, atendendo aos índices estabelecidos neste instrumento convocatório.

17.5.8. PATRIMÔNIO LÍQUIDO MÍNIMO não inferior a 10% da estimativa de custos da licitação, que deverá ser comprovado através da apresentação do balanço patrimonial.

17.6. REGULARIDADE FISCAL E TRABALHISTA

17.6.1 - PROVA DE REGULARIDADE PARA COM AS FAZENDAS FEDERAL, ESTADUAL e MUNICIPAL da sede ou filial do licitante, expedidos pelos órgãos abaixo relacionados e dentro dos seus períodos de validade, devendo os mesmos apresentar igualdade de CNPJ.

a. CERTIDÃO NEGATIVA DE DÉBITOS RELATIVOS A CRÉDITOS TRIBUTÁRIOS FEDERAIS E Á DIVIDA ATIVA DA UNIÃO, OU EQUIVALENTE, EXPEDIDA PELA PROCURADORIA GERAL DA FAZENDA NACIONAL E RECEITA FEDERAL DO BRASIL.

b. CERTIDÃO NEGATIVA DE DÉBITOS ESTADUAIS, OU EQUIVALENTE, EXPEDIDA PELA SECRETARIA DA FAZENDA DO ESTADO.

c. CERTIDÃO NEGATIVA DE DÉBITOS MUNICIPAIS, OU EQUIVALENTE, EXPEDIDA PELA SECRETARIA DE FINANÇAS DO MUNICÍPIO SEDE DA LICITANTE.

17.6.2 - CERTIFICADO DE REGULARIDADE DE SITUAÇÃO (CRS) OU EQUIVALENTE, perante o Gestor do Fundo de Garantia por Tempo de Serviço (**FGTS**), da jurisdição da sede ou filial do licitante, devendo o mesmo ter igualdade de CNPJ com os demais documentos apresentados na comprovação da regularidade fiscal.

17.6.3 - No caso de cooperativa, a mesma está dispensada da apresentação dos documentos relativos ao FGTS dos cooperados, para efeito desta dispensa, deverá apresentar o seguinte:

a. DECLARAÇÃO constando que, caso vencedor da licitação, o objeto será produzido ou comercializado por ela própria através de seus cooperados.

b. ATA DA SESSÃO em que os cooperados autorizaram a cooperativa a participar da licitação e executar o contrato caso seja vencedora.

c. RELAÇÃO DOS COOPERADOS que produzirão ou comercializarão o objeto da licitação discriminado, comprovando através de documento a data de ingresso de cada um deles na cooperativa.

17.6.4 – Caso a cooperativa tenha empregados em seus quadros, esta deverá juntar os documentos comprobatórios de recolhimento do FGTS relativo a eles.

17.6.5 – Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa, ou positiva com efeitos de negativa, nos termos do título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1ª de maio de 1943.

17.6.6 - O licitante deverá apresentar documento relativo ao cumprimento do disposto no inciso XXXIII, do art. 7º, da Constituição Federal e na Lei Federal nº 9.854/1999 conforme Anexo F - Declaração Relativa ao Trabalho de Empregado Menor.

18. OUTRAS DISPOSIÇÕES

18.1 A não comprovação da regularidade fiscal e trabalhista, até o final do prazo estabelecido, implicará na decadência do direito, sem prejuízo das sanções cabíveis, sendo facultado ao pregoeiro convocar os licitantes remanescentes, por ordem de classificação.

19. DOS BENEFÍCIOS PARA ME E EPP:

19.1. Será garantida aos licitantes enquadrados como microempresas, empresas de pequeno porte e as cooperativas, que se enquadrem nos termos do art. 34, da Lei Federal nº 11.488/2007, como critério de desempate, preferência de contratação, o previsto na Lei Complementar n° 123/2006, em seu Capítulo V – DO ACESSO AOS MERCADOS / DAS AQUISIÇÕES PÚBLICAS e alterações previstas na Lei Complementar n° 147 de 07/08/2014.

19.2. Havendo restrição quanto à regularidade fiscal e trabalhista da microempresa, da empresa de pequeno porte ou da cooperativa que se enquadre nos termos do art. 34, da Lei Federal nº 11.488/2007, será assegurado o prazo de 5 (cinco) dias úteis, contados da declaração do vencedor, para a regularização do(s) documento(s), podendo tal prazo ser prorrogado por igual período, conforme dispõe a Lei Complementar nº 123/2006 e alterações na Lei Complementar n° 147 de 07/08/2014, Lei Municipal 10.350 de 28/05/2015, e Decreto Municipal n° 13.735 de 18/01/2016.

19.3 Da NÃO destinação de LOTE para MEI, ME E EPP:

19.3.1 Conforme justificativa técnica emitida pela Coordenadoria de Gestão Corporativa de Tecnologia da Informação – COGECT, não será destinado lote exclusivo a MEI, ME E EPP, em conformidade com o art. 49, III, da Lei Complementar Federal 123/2006, art. 35, II, da Lei Municipal nº 10.350/2015 e art. 36, II, do Decreto Municipal nº 13.735/2016

20. DOS CRITÉRIOS DE JULGAMENTO

20.1. Para julgamento das propostas será adotado o critério de **MENOR PREÇO**, observado o estabelecido nas condições definidas neste edital e o disposto no Mapa de Preços que norteia a contratação, tomando-se como parâmetro, para tanto, o menor preço coletado, na sequência, ou a média de preços, sempre buscando alcançar a maior vantajosidade.

20.1.1. A disputa será realizada por lote, sendo os preços registrados em ata, pelo valor unitário do item.

20.1.2.**A proposta final para o lote não poderá conter item com valor superior ao estimado pela administração, sob pena de desclassificação.**

20.1.3. Na fase de lances, o lance final deverá atingir preço igual ou inferior ao limite máximo constante daquele mapa de preços. Caso não seja realizada a fase de lances, o licitante que cotou na proposta o menor preço deverá reduzi-lo a um valor igual ou inferior ao limite máximo do referido mapa de preços.

20.1.4. Se a proposta de menor preço não for aceitável, ou, ainda, se o licitante desatender às exigências habilitatórias, o pregoeiro examinará a proposta subsequente, verificando sua compatibilidade e a habilitação do participante, na ordem de classificação, e assim sucessivamente, até a apuração de uma proposta que atenda a este edital.

20.1.5. O licitante remanescente que esteja enquadrado no percentual estabelecido no art. 44, § 2º, da Lei Complementar nº 123/2006, no dia e hora designados pelo pregoeiro, será convocado na ordem de classificação, no "chat de mensagem", para ofertar novo lance inferior ao melhor lance registrado no lote, para, no prazo de 5 (cinco) minutos, utilizar-se do direito de preferência, observando o item 12.6.1

21. SERÃO DESCLASSIFICADAS AS PROPOSTAS DE PREÇOS:

21.1. Em condições ilegais, omissões, ou conflitos com as exigências deste edital.

21.2. Com preços superiores dos ITENS/LOTES aos constantes no mapa de preços no processo em epígrafe, após a fase de lances ou comprovadamente inexequíveis.

21.2.1. Considera-se manifestamente inexequível a proposta de preços que, comprovadamente, for insuficiente para a cobertura dos custos da contratação, resulte preço global ou unitários simbólicos, irrisórios ou de valor zero, incompatíveis com os preços dos insumos e tarifas de mercado, acrescidos dos respectivos encargos, ainda que o ato convocatório da licitação não tenha estabelecido preços mínimos.

21.2.2. Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderão ser efetuadas diligências, na forma do § 3° do artigo 43 da Lei n° 8.666, de 1993.

21.2.3. Quando o licitante apresentar preço final inferior a 30% (trinta por cento) da média dos preços ofertados, não sendo possível a sua imediata desclassificação por inexequibilidade, será obrigatória a realização de diligências para o exame da proposta.

21.3. A desclassificação será sempre fundamentada e registrada no sistema.

22. DOS PEDIDOS DE ESCLARECIMENTOS E IMPUGNAÇÕES

22.1. Os pedidos de esclarecimentos referentes ao processo licitatório deverão ser enviados ao pregoeiro, até 3 (três) dias úteis anteriores à data fixada para abertura das propostas, exclusivamente por meio eletrônico, no endereço **licitacao@fortaleza.ce.gov.br**, informando o número deste pregão no sistema do Banco do Brasil e o órgão interessado.

22.2. Nos pedidos de esclarecimentos encaminhados, os interessados deverão se identificar (CNPJ, Razão Social e nome do representante que pediu esclarecimentos, se pessoa jurídica e CPF para pessoa física) e disponibilizar as informações para contato (endereço completo, telefone, fax e e-mail).

22.3. Os esclarecimentos serão prestados pelo Pregoeiro, por escrito, por meio de e-mail àqueles que enviaram solicitações.

22.4. Até 2 (dois) dias úteis antes da data fixada para abertura das propostas, qualquer pessoa poderá impugnar o presente edital, mediante petição por escrito, protocolada na Central de Licitações da Prefeitura de Fortaleza - CLFOR, no endereço constante no subitem 9.1 deste edital.

22.6. As respostas aos pedidos de impugnações e esclarecimentos aderem a esse Edital tal como se dele fizessem parte, vinculando a Administração e os licitantes.

22.7. Qualquer modificação no Edital exige divulgação pelo mesmo instrumento de publicação em que se deu o texto original, reabrindo-se o prazo inicialmente estabelecido, exceto quando, inquestionavelmente, a alteração não afetar a formulação das propostas.

22.8. Não serão conhecidas as impugnações apresentadas fora do prazo legal e/ou subscritas por representante não habilitado legalmente exceto se tratar de matéria de ordem pública.

22.9. Caberá ao pregoeiro, auxiliado pela área interessada, quando for o caso, enviar a petição de impugnação para que a autoridade competente decida no prazo de 24 (vinte e quatro) horas.

22.10. Acolhida a impugnação contra o edital, será designada nova data para a realização do certame, exceto se a alteração não afetar a formulação das propostas.

23. DOS RECURSOS ADMINISTRATIVOS

23.1. Declarado vencedor, qualquer licitante poderá manifestar, de forma imediata e motivada, a intenção de interpor recurso contra ato do pregoeiro, em campo próprio do sistema, quando lhe será concedido o prazo de 3 (três) dias para apresentação das razões por escrito, devidamente protocolizadas na Central de Licitações da Prefeitura de Fortaleza - CLFOR, no endereço constante no **subitem 9.1** deste edital. Os demais licitantes ficam desde logo convidados a apresentar contrarrazões dentro de igual prazo, que começará a contar a partir do término do prazo do recorrente, sendo-lhes assegurado vista imediata dos autos.

23.2. Não serão conhecidos os recursos intempestivos e/ou subscritos por representante não habilitado legalmente ou não identificado no processo licitatório para responder pelo proponente.

23.3. A falta de manifestação, conforme o **subitem 23.1** deste edital importará na decadência do direito de recurso.

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

23.5. A decisão em grau de recurso será definitiva, e dela dar-se-á conhecimento aos licitantes, no endereço eletrônico constante no **subitem 7.2**. deste edital.

24. DA ADJUDICAÇÃO E DA HOMOLOGAÇÃO

24.1. A adjudicação dar-se-á pelo pregoeiro quando não ocorrer interposição de recursos. Caso contrário, a adjudicação ficará a cargo da autoridade competente.

24.2. A homologação da licitação é de responsabilidade da autoridade competente e só poderá ser realizada depois da adjudicação do objeto ao vencedor.

24.3. No caso de interposição de recurso, sendo a adjudicação da competência do titular da origem desta licitação, decidido o recurso, este homologará o julgamento do Pregoeiro e adjudicará o objeto ao vencedor.

24.4. O titular da origem desta licitação se reserva o direito de não homologar ou revogar o presente processo por razões de interesse público decorrente de fato superveniente devidamente comprovado e mediante fundamentação escrita.

24.5. O sistema gerará ata circunstanciada, na qual estarão registrados todos os atos do procedimento e as ocorrências relevantes.

25. DAS SANÇÕES ADMINISTRATIVAS

25.1. O licitante que praticar ato ilícito, dentre os quais os previstos no art. 7º da Lei Federal nº 10.520/2002, como: não assinar a Ata de Registro de Preços e, no caso da Detentora não celebrar o contrato, estando convocado dentro do prazo de validade da sua proposta; deixar de entregar ou apresentar documentação falsa exigida para o certame; ensejar o retardamento da execução de seu objeto; não mantiver a proposta; falhar ou fraudar na execução do contrato; comportar-se de modo inidôneo; fizer declaração falsa ou cometer fraude fiscal; garantido o direito prévio de citação e da ampla defesa, sem prejuízo das sanções legais nas esferas civis e criminais, estará sujeito às seguintes penalidades, de acordo com o Decreto Municipal nº 13.735/2016:

I. Advertência, que consista em comunicação formal ao infrator, decorrente da inexecução de deveres que ocasionem riscos e/ou prejuízos de menor potencial ofensivo para a Administração;

II. Multa cumulativa com as demais sanções, conforme estabelecido nos artigos 50 e 51 do Decreto Municipal nº 13.375/2016

III. Impedimento de licitar e contratar com a Administração Direta e Indireta do Município de Fortaleza e descredenciamento no Cadastro de Fornecedores da Central de Licitações da Prefeitura de Fortaleza - CLFOR, pelo prazo de até 05 (cinco) anos.

25.1.1. Entende-se por ato ilícito qualquer conduta comissiva ou omissiva que infrinja dispositivos legais ou regras constantes de regulamentos ou de qualquer outro ato normativo, inclusive aquelas constantes dos atos convocatórios de licitação, da ata de registro de preços, do contrato ou instrumento que o substitua.

25.1.2. A aplicação das multas de natureza moratória não impede a aplicação superveniente de outras multas previstas neste item, cumulando-se os respectivos valores.

25.1.3. O atraso, para efeito de cálculo da multa, será contado em dias corridos, a partir do primeiro dia útil subsequente ao do encerramento do prazo estabelecido para o cumprimento da obrigação

25.1.4. Após esgotados os meios de execução direta da sanção de multa, o licitante será notificado para recolher a importância devida no prazo de 15 (quinze) dias, contados do recebimento da

comunicação oficial. Decorrido o prazo, a CLFOR encaminhará a multa para que seja inscrita na Dívida Ativa do Município.

25.2. Na aplicação das sanções devem ser consideradas as seguintes circunstancias:

I. a natureza e a gravidade da infração cometida;

II. os danos que o cometimento da infração ocasionar aos serviços e aos usuários;

III. a vantagem auferida em virtude da infração;

IV. as circunstancias gerais agravantes e atenuantes;

V. os antecedentes da licitante ou contratada.

26. DA CONTRATAÇÃO

26.1. A adjudicatária terá o prazo de 5 (cinco) dias úteis, contados a partir da convocação, para a assinatura do contrato. Este prazo poderá ser prorrogado uma vez por igual período, desde que solicitado durante o seu transcurso e, ainda assim, se devidamente justificado e aceito.

26.2. Na assinatura do contrato será exigida a comprovação das condições de habilitação exigidas neste edital, as quais deverão ser mantidas pela contratada durante todo o período da contratação.

26.2.1. Se, por ocasião da formalização do contrato, as certidões de regularidade de débito da Adjudicatária perante o Sistema de Seguridade Social (INSS), o Fundo de Garantia por Tempo de Serviço (FGTS), a Fazenda Nacional, Estadual, Municipal e Justiça do Trabalho (CNDT), estiverem com os prazos de validade vencidos, o órgão licitante verificará a situação por meio eletrônico hábil de informações, certificando nos autos do processo a regularidade e anexando os documentos passíveis de obtenção por tais meios, salvo impossibilidade devidamente justificada;

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

26.3. Quando a adjudicatária não comprovar as condições habilitatórias consignadas neste edital, ou recusar-se a assinar o contrato, poderá ser convidado outro licitante pelo pregoeiro, desde que respeitada a ordem de classificação, para, depois de comprovados os requisitos habilitatórios e feita a negociação, assinar o contrato.

26.4. Para fins de contratação, a licitante vencedora que recolha encargos sociais ou tributos diferenciados, deverá informar a CONTRATANTE quando da assinatura do contrato.

26.5. A forma de pagamento, prazo contratual, reajuste, recebimento e demais condições aplicáveis à contratação estão definidas no Anexo A – Termo de Referência e no Anexo E – Minuta do Contrato, parte deste edital.

27. DA GARANTIA CONTRATUAL:

27.1. Após a adjudicação do objeto do certame e até a data da contratação ou em outro prazo solicitado formalmente pelo licitante vencedor, aceito e/ou estipulado pela Administração, o licitante vencedor deverá prestar garantia contratual correspondente a 5% (cinco por cento) sobre o valor do contrato, em conformidade com o disposto no art. 56 da Lei Federal nº 8.666/1993, vedada a prestação de garantia através de Títulos da Dívida Agrária.
27.2. Na garantia deverá estar expresso prazo de validade superior a 90 (noventa) dias do prazo de vigência do contrato.
27.3. A garantia prestada será restituída e/ou liberada após o cumprimento integral de todas as obrigações contratuais e, quando em dinheiro, será atualizada monetariamente, conforme dispõe o § 4º, do art. 56, da Lei Federal nº 8.666/1993.
27.4. A não prestação de garantia equivale à recusa injustificada para a contratação, caracterizando descumprimento total da obrigação assumida, ficando a adjudicatária sujeita às penalidades legalmente estabelecidas, inclusive multa.
27.5. Na ocorrência de acréscimo contratual de valor, deverá ser prestada garantia proporcional ao valor acrescido, nas mesmas condições estabelecidas no subitem 27.1.

28. DAS DISPOSIÇÕES GERAIS

28.1. Esta licitação não importa, necessariamente, em contratação, podendo a autoridade competente revogá-la por razões de interesse público, anulá-la por ilegalidade de ofício ou por provocação de terceiros, mediante decisão devidamente fundamentada, sem quaisquer reclamações ou direitos à indenização ou reembolso.
28.2. É facultada ao pregoeiro ou à autoridade superior, em qualquer fase da licitação, a promoção de diligência destinada a esclarecer ou a complementar a instrução do processo licitatório, vedada a inclusão posterior de documentos que deveriam constar originariamente na proposta e na documentação de habilitação.
28.3. Quando todas as propostas de preços escritas forem desclassificadas, é facultado ao Titular do órgão de origem do processo fixar o prazo de 08 (oito) dias úteis para a apresentação de novas propostas escoimadas exclusivamente nas causas que provocaram a desclassificação.
28.4. O descumprimento de prazos estabelecidos neste edital e/ou pelo pregoeiro ou o não atendimento às solicitações ensejará DESCLASSIFICAÇÃO ou INABILITAÇÃO.
28.5. Toda a documentação fará parte dos autos e não será devolvida ao licitante, ainda que se trate de originais.
28.6. Na contagem dos prazos estabelecidos neste edital excluir-se-ão os dias de início e incluir-se-ão os dias de vencimento. Os prazos estabelecidos neste edital se iniciam e se vencem em dias úteis.
28.7. Os licitantes são responsáveis pela fidelidade e legitimidade das informações e dos documentos apresentados em qualquer fase da licitação.
28.8. O desatendimento de exigências formais não essenciais não implicará no afastamento do licitante, desde que seja possível a aferição da sua qualificação e a exata compreensão da sua proposta.

28.9. Toda a documentação exigida deverá ser apresentada em original ou por qualquer processo de reprografia autenticada, inclusive pelo pregoeiro. Caso esta documentação tenha sido emitida pela internet, só será aceita após a confirmação de sua autenticidade.
28.10. O pregoeiro poderá sanar erros formais que não acarretem prejuízos para o objeto da licitação, para a Administração e para os licitantes, dentre estes, os decorrentes de operações aritméticas.
28.11. Os casos omissos serão resolvidos pelo pregoeiro, nos termos da legislação pertinente.
28.12. Todas e quaisquer comunicações com o Pregoeiro dar-se-ão por escrito, com o devido protocolo na sede da Central de Licitações da Prefeitura de Fortaleza - CLFOR, ou por meio de fac símile para o número (85) 3252.1630, ou via e-mail institucional **licitacao@fortaleza.ce.gov.br**, ou no próprio chat da plataforma do Banco do Brasil "sala virtual" em que estará acontecendo o certame.
28.13. É vedado ao Pregoeiro, sob qualquer hipótese ou pretexto, prestar quaisquer informações sobre pregão já publicado e/ou em andamento, usando telefonia fixa ou móvel, como forma de garantir a lisura do certame.
28.14. As normas que disciplinam este pregão serão sempre interpretadas em favor da ampliação da disputa.
28.15. A apresentação, por parte dos licitantes, de DECLARAÇÃO FALSA relativa ao cumprimento dos requisitos de habilitação, aos impedimentos de participação ou ao enquadramento como microempresa ou empresa de pequeno porte sujeitará o licitante às sanções previstas neste Edital, e art. 37 da Lei Complementar nº 123/2006, independentemente da adoção de providências quanto à responsabilização penal, com fundamento no art. 90 da Lei nº 8.666/93 e art. 299 do Código Penal Brasileiro.
28.16. Serão consideradas como não apresentadas as declarações não assinadas pelo representante legal da empresa ou seu procurador. Diante da ausência de assinatura, será desclassificada a proposta ou inabilitada a empresa, conforme a fase em que a declaração deva ser apresentada.
28.17. O foro designado para julgamento de quaisquer questões judiciais resultantes deste edital será o da Comarca de Fortaleza, Capital do Estado do Ceará.

29. DOS ANEXOS

29.1. Constituem anexos deste edital, dele fazendo parte:

ANEXO A – TERMO DE REFERÊNCIA
ANEXO B – MODELO DA PROPOSTA DE PREÇOS
ANEXO C – MODELO MERAMENTE SUGESTIVO DE DECLARAÇÃO DE MICROEMPRESA, EMPRESA DE PEQUENO PORTE OU COOPERATIVA (*entregar junto com a proposta de preços escrita*)
ANEXO D - MODELO DE DECLARAÇÃO DE CONTRATOS FIRMADOS COM A INICIATIVA PRIVADA E ADMINISTRAÇÃO PÚBLICA
ANEXO E – MINUTA DO CONTRATO

ANEXO F – DECLARAÇÃO RELATIVA AO TRABALHO DE EMPREGADO MENOR
ANEXO G– MODELO DE ORDEM DE SERVIÇO
ANEXO H – ANÁLISE DAS AMOSTRAS
ANEXO I - GLOSSÁRIO

CIENTE:

Philipe Theophilo Nottingham
SECRETÁRIO MUNICIPAL DO PLANEJAMENTO, ORÇAMENTO E GESTÃO

Aprovação expressa da assessoria jurídica:

Airton Douglas de Andrade Lucas
Coordenador Jurídico
OAB/CE nº 17.404
Coordenadoria Jurídica - COJUR/SEPOG

ANEXO A - TERMO DE REFERÊNCIA

1. UNIDADE REQUISITANTE:

SECRETARIA MUNICIPAL DO PLANEJAMENTO, ORÇAMENTO E GESTÃO - SEPOG

2. DO OBJETO:

CONSTITUI OBJETO DA PRESENTE LICITAÇÃO A CONTRATAÇÃO DE EMPRESA ESPECIALIZADA NO FORNECIMENTO DE SOLUÇÃO INTEGRADA DE SEGURANÇA DE PERÍMETRO (FIREWALL), QUE POSSIBILITE A VISIBILIDADE E CONTROLE DE TRÁFEGO, FILTRAGEM DE CONTEÚDO WEB, PREVENÇÃO CONTRA AMEAÇAS DE REDES MODERNAS, FILTRO DE DADOS, VPN E CONTROLE GRANULAR DE BANDA DE REDE, COMPREENDENDO FORNECIMENTO DE EQUIPAMENTOS E SOFTWARES INTEGRADOS, *APPLIANCE*, LICENCIAMENTO E GARANTIA DE ATUALIZAÇÃO PARA ATENDER AS NECESSIDADES DA PREFEITURA MUNICIPAL DE FORTALEZA, DE ACORDO COM AS ESPECIFICAÇÕES E QUANTITATIVOS CONTIDOS NO ANEXO A – TERMO DE REFERÊNCIA DESTE EDITAL, PARA O PERÍODO DE 12 MESES.

3. DA JUSTIFICATIVA TÉCNICA DA LICITAÇÃO:

Fortaleza possui uma das maiores redes públicas de fibra ótica do País, com 240 quilômetros que conectam 92 unidades da administração direta e indireta do Município. Em 2013, quando se deu início a implantação dessa rede, a administração passou a contar com conexão mais segura e de melhor qualidade e velocidade.

Esse trabalho faz parte do processo de modernização administrativa pela qual a atual gestão tem se pautado. O caminho ideal é que todos os órgãos/unidades da Prefeitura Municipal de Fortaleza (PMF) estejam conectados e possam se comunicar entre si, gerando informações mais confiáveis, melhor navegabilidade e mais economia para a administração.

Diante disso, a PMF planeja expandir sua rede de fibra óptica (FIBRAFOR) para 870 km de extensão, integrando também escolas e postos de saúde de modo que facilitem as ações, projetos e rotinas de gestão, especialmente aquelas voltadas para gestão do patrimônio, de aquisições, logística e de pessoas.

O Projeto de expansão da FIBRAFOR prevê a integração de 110 unidades de saúde e 483

unidades de educação. A inserção dessas unidades resultará em um grande ganho para gestão, visto que, atualmente, a estrutura de link de Internet da Prefeitura é centralizada e possui uma velocidade de 2 Gbps que é compartilhada entre seus órgãos. Esse link foi segmentado para formar a estrutura redundante, mantendo-se 1Gbps na Secretaria de Finanças do Município; 750 Mbps na Secretaria do Planejamento, Orçamento e Gestão e 250 Mbps no Hospital e Maternidade Dra. Zilda Arns Neumann. Deste modo, quando um link se torna indisponível, o outro assume a Internet automaticamente, garantindo mais acessibilidade aos sistemas governamentais.

Manter todas as unidades municipais integradas a uma fibra de qualidade é fundamental para os projetos de melhoria da gestão que a Secretaria do Planejamento, Orçamento e Gestão (SEPOG) pretende implementar nesse ano de 2017 e isso inclui a necessidade de absorver as unidades educacionais e de saúde.

Para que essa gestão seja bem-feita é imprescindível que as escolas e postos de saúde tenham disponível uma rede de conectividade com um perfil aceitável de navegabilidade e segurança

Garantir a eficiência do gasto público é o que a PMF tem buscado continuamente e a inserção dessas unidades trará maior eficiência para a administração. Para que isso aconteça é necessário a aquisição de solução integrada de segurança de perímetro (Firewall) para integrar esses 593 novos pontos e garantir a segurança da informação, minimizando os riscos segurança, de violação de dados e informações.

Considerando todas as integrações a serem realizadas, a Prefeitura Municipal de Fortaleza – PMF, por intermédio da SEPOG/COGECT, com o projeto FIBRAFOR realiza a conexão da maioria dos órgãos e entidades da administração pública do município de Fortaleza. Desta forma, visando a melhoria continua no fornecimento deste serviço, faz-se necessário a aquisição de equipamentos de informática para garantir a segurança das interconexões entre as unidades municipais da PMF. Faz-se a aquisição da solução de segurança, ser de suma importância para a proteção dos dados que trafegam na rede corporativa da Prefeitura Municipal de Fortaleza.

Com a integração das 593 novas unidades, distribuídas entre unidades educacionais e de saúde, é imprescindível a aquisição de uma solução de segurança da informação de perímetro mais robusta. Assim, quanto mais Órgãos trafegando na Rede Corporativa, maior é a necessidade de um equipamento com mais capacidade de análise dos dados trafegados na borda da rede e que escoe todo o tráfego de saída de internet desses Órgãos possibilitando analisar, proteger e, ainda:

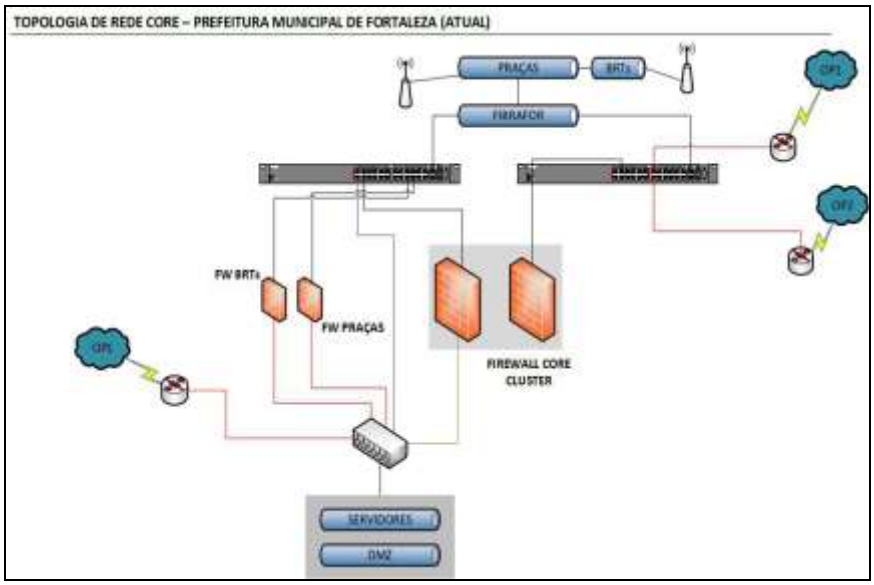
- Configurar filtros para bloqueio dos conteúdos impróprios;
- Emitir relatórios dos acessos realizados por IP;
- Definir políticas para proteção da rede contra: ataques internos e ou externos, regras de bloqueio e liberação de serviços e portas TCP e UDP, bloqueio mensagens instantâneas, e ou aplicações que venha a impactar na performance e na segurança da rede, fechamento de portas não utilizadas, possibilitar o controle da velocidade de banda, a fim de evitar abusos nos recursos de rede e evitar impacto na qualidade do serviço;
- Proteção do Parque Tecnológico (DATA CENTER), uma vez que estará minimizado os ataques descritos acima;
- Criar conexões seguras e Criptografadas, para garantir a confidencialidade dos dados que nelas trafegarem - VPNs
- Garantir a disponibilidade de link para internet, via Failover e / ou *LoadBalance*;
- Monitorar links de dados.

O Firewall auxilia no combate a infestações de pragas digitais, tais como cavalos de troia, vírus, *worms*, diversos tipos de *malwares*. Para auxiliar neste combate, o firewall bloqueia as portas que eventualmente são utilizadas por estas pragas, impedindo assim, sua proliferação.

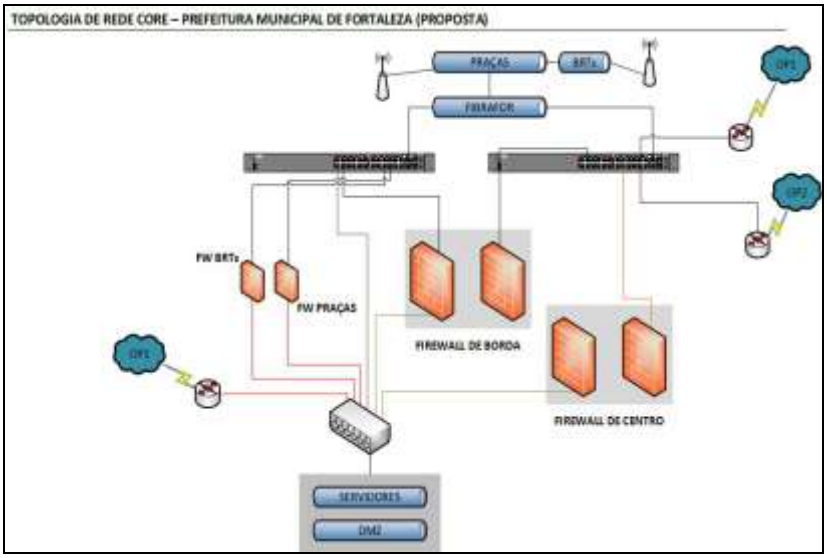
Desta forma, a aquisição de firewall e softwares que o gerencie se justifica pelos fatores acima descritos, proporcionando diversos benefícios à PMF.

Em nossa proposta, utilizaremos a nova solução de segurança em conjunto com a solução atual, conforme figuras abaixo:

- Figura 1



- Figura 2



Frise-se, por oportuno, que o produto necessita de uma garantia de 36 meses, conforme as especificações do Termo de Referência, tendo em vista que tal equipamento será responsável pelo combate a infestações de pragas digitais, tais como cavalos de troia, vírus, worms, diversos tipos de malwares, garantindo a segurança e continuidade dos serviços da PMF.

Diante do exposto, justifica-se a contratação de uma empresa especializada para a aquisição de solução de segurança de perímetro - firewall, atendendo ao projeto de expansão da rede óptica metropolitana de Fortaleza, por meio de processo licitatório, devendo ser observadas as normas e

condições do Edital e as disposições contidas na Lei Federal nº 10.520, de 17 de julho 2002, Lei Complementar nº 123, de 14 de dezembro de 2006, Lei Complementar nº 147 de 07 de agosto de 2014, nos Decretos Municipais nºs 11.251 de 10 de setembro de 2002, nº 13.512 de 30 de dezembro de 2014, n° 13.735 de 18 de janeiro de 2016 e subsidiariamente a Lei Federal nº. 8.666, de 21 de junho de 1993, com suas alterações.

4. CLASSIFICAÇÃO DOS BENS E SERVIÇOS COMUNS:

Os serviços a serem contratados enquadram-se na classificação de serviços comuns, nos termos da Lei 10.520/02, do Dec. 3.555/00 e do Dec. 5.450/05.

5. DA MODALIDADE:

Este objeto será realizado através de licitação na modalidade PREGÃO, na forma ELETRÔNICA, do tipo MENOR PREÇO, com a forma de fornecimento de forma integral.

6. DAS ESPECIFICAÇÕES E QUANTITATIVOS:

6.1. Sob pena de desclassificação, os licitantes deverão apresentar suas propostas, obedecendo as especificações técnicas, bem como requisitos mínimos exigidos neste anexo.

LOTE ÚNICO		
ITEM	**DESCRIÇÃO**	**QUANTIDADE**
01	Solução de alta disponibilidade de *Next Generation Firewall*, com garantia de funcionamento, atualização de assinaturas de proteção e suporte técnico local e remota, 24x7, pelo prazo de 36 meses (trinta e seis) meses, incluindo serviços de instalação.	01

7. DETALHAMENTO DAS ESPECIFICAÇÕES TÉCNICAS MÍNIMAS

7.1. CARACTERÍSTICAS GERAIS

7.1.1. Prover solução de segurança perimetral que inclui Firewall de Próxima Geração com Controle de Ameaças Avançadas, com desempenho suficiente para suportar a ativação e configuração simultânea de todas as funcionalidades e recursos descritos neste termo para os valores de desempenho descritos;

7.1.2. As funcionalidades de segurança descritas nesta especificação devem ser disponibilizadas em hardware do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;

7.1.3. As funcionalidades de proteção de rede que compõe a plataforma de segurança devem funcionar no mesmo appliance, não sendo aceito soluções onde aja a necessidade da combinação de múltiplos dispositivos para composição da solução de segurança ofertada;

7.1.4. Todo o ambiente deverá ser gerenciado através de uma única interface do próprio fabricante da solução, sem a necessidade de produtos de terceiros para compor a solução;

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

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

7.1.7. A gerência poderá ser virtualizada, desde que compatível com as plataformas de virtualização da VMware e/ou Hyper-V e/ou RHEV, ou fornecida em hardware do tipo appliance;

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

7.1.9. O software da solução de segurança deverá ser fornecido em sua versão mais atual e estável possível, até a data de publicação deste certame, não sendo permitido qualquer tipo de comprovação futura e/ou versões que não estejam publicadas em sua versão final no site do próprio fabricante, não sendo aceitos também versões experimentais, versões de teste e/ou customizadas para clientes específicos;

7.1.10. A solução de segurança deve incluir todas as licenças necessárias para o perfeito funcionamento de todas as funcionalidades descritas nesta especificação por 03 (três) anos, incluindo a atualização de sua base de assinaturas;

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

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

7.2. REQUISITOS MÍNIMOS

7.2.1. Suporte a 4094 VLAN Tags 802.1q;

3.2.2 Agregação de links 802.3ad e LACP;

3.2.3 Policy based routing ou policy based forwarding;

3.2.4 Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e/ou PIM-DM);

3.2.5 Suporte a DHCP Relay;

3.2.6 Suporte a DHCP Server;

3.2.7 Suporte a Jumbo Frames;

3.2.8 Deve suportar os seguintes tipos de NAT:

3.2.8.1 Deve suportar NAT dinâmico (Many-to-1);
3.2.8.2 Deve suportar NAT dinâmico (Many-to-Many);
3.2.8.3 Deve suportar NAT estático (1-to-1);
3.2.8.4 Deve suportar NAT estático (Many-to-Many);
3.2.8.5 Deve suportar NAT estático bidirecional 1-to-1;
3.2.8.6 Deve suportar Tradução de porta (PAT);
3.2.8.7 Deve suportar NAT de Origem;
3.2.8.8 Deve suportar NAT de Destino;
3.2.8.9 Deve suportar NAT de Origem e NAT de Destino simultaneamente;
3.2.8.10 Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
3.2.8.11 Deve suportar NAT64;
3.2.8.12 Deve implementar o protocolo ECMP;
3.2.8.13 Deve implementar balanceamento de link por hash do IP;
3.2.8.14 Deve implementar balanceamento de link através do método round-robin;
3.2.8.15 Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, três links;
3.2.8.16 Deve implementar balanceamento de link através de políticas por aplicação e/ou porta de destino;
3.2.8.17 Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais
3.2.8.18 Deve permitir monitorar via SNMP falhas de hardware, uso de recursos por número elevado de sessões, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster, ataques e estatísticas de uso das interfaces de rede
3.2.8.19 Enviar log para sistemas de monitoração externos, simultaneamente;
3.2.8.20 Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;
3.2.8.21 Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;
3.2.8.22 Proteção contra anti-spoofing;
3.2.8.23 Para IPv4, deve suportar roteamento estático e dinâmico:
3.2.8.23.1 RIPv2;
3.2.8.23.2 BGP;
3.2.8.23.3 OSPFv2.
3.2.8.24 Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);
3.2.8.25 Suportar OSPF graceful restart;
3.2.8.26 Os dispositivos de proteção devem ter a capacidade de operar de forma simultânea em uma única instância de firewall, mediante o uso de suas interfaces físicas nos seguintes modos: Modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3);
3.2.8.27 Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
3.2.8.28 Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;

3.2.8.29 Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha visibilidade do tráfego;

3.2.8.30 Deve suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;

3.2.8.31 Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo:

3.2.8.31.1 Em modo transparente;

3.2.8.31.2 Em layer 3;

3.2.8.31.3 Em layer 3 e com no mínimo 2 equipamentos no cluster.

3.2.8.32 A configuração em alta disponibilidade deve sincronizar:

3.2.8.32.1 Sessões;

3.2.8.32.2 Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede;

3.2.8.32.3 Associações de Segurança das VPNs;

3.2.8.32.4 Tabelas FIB;

3.2.8.32.5 Certificados de-criptografados;

3.2.8.32.6 Associações de Segurança das VPNs;

3.2.8.33 Os dispositivos de proteção de rede devem suportar subinterfaces ethernet logicas

3.2.8.34 O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link;

3.2.8.35 Deve possuir suporte à criação de sistemas virtuais no mesmo appliance;

3.2.8.36 Em alta disponibilidade, deve ser possível o uso de clusters virtuais, seja ativo-ativo ou ativo-passivo, permitindo a distribuição de carga entre diferentes contextos;

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

3.2.8.38 Controle, inspeção e descriptografia de SSL para tráfego de entrada (Inbound) e Saída (Outbound).

7.3.REQUISITOS POR FUNCIONALIDADE

7.4.3. CONTROLE POR POLÍTICA DE FIREWALL

7.3.1.1 Deverá suportar controles por zona ou grupo de segurança

7.3.1.2. Controles de políticas por porta e protocolo

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

7.3.1.4. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas ou grupo de segurança

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

7.3.1.6. Deve suportar offload de certificado em inspeção de conexões SSL de entrada (Inbound);

7.3.1.7. Deve descriptografar tráfego Inbound e Outbound em conexões negociadas

com TLS 1.2;

7.3.1.8. Controle de inspeção e descriptografia de SSH por política;

7.3.1.9. Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada;

7.3.1.10. Traffic shaping QoS baseado em Políticas (Prioridade, Garantia e Máximo);

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

7.3.1.12. Suporte a objetos e regras IPV6;

7.3.1.13. Suporte a objetos e regras multicast;

7.3.1.14. Deve suportar no mínimo três tipos de resposta nas políticas de firewall:

7.3.1.15. Drop sem notificação do bloqueio ao usuário;

7.3.1.16. Drop com notificação do bloqueio ao usuário;

7.3.1.17. Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego, TCP-Reset para o client, TCP-Reset para o server ou para os dois lados da conexão;

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

7.4. CONTROLE DE APLICAÇÕES

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

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

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

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

7.4.5. Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;

7.4.6. Deve detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a bittorrent e aplicações VoIP que utilizam criptografia proprietária;

7.4.7. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede ToR

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

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

7.4.10. Identificar o uso de táticas evasivas via comunicações criptografadas;

7.4.11. Atualizar a base de assinaturas de aplicações automaticamente;

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

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

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

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

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

7.4.17. Permitir a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias sem a necessidade de ação do fabricante

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

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

7.4.20. Deve alertar o usuário quando uma aplicação for bloqueada;

7.4.21. Deve possibilitar a diferenciação de tráfegos Peer-to-Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;

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

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

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

7.4.25. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc.)

7.4.26. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Nível de risco da aplicação

7.4.27. Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação

7.5. PREVENÇÃO DE AMEAÇAS AVANÇADAS

7.5.1. Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de Firewall;

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

7.5.3. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;

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

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

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

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

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

7.5.9. Deve permitir o bloqueio de vulnerabilidades

7.5.10. Deve permitir o bloqueio de exploits conhecidos

7.5.11. Deve incluir proteção contra-ataques de negação de serviços

7.5.12. Deverá possuir o seguinte mecanismos de inspeção de IPS: Análise de padrões de estado de conexões;

7.5.13. Deverá possuir o seguinte mecanismos de inspeção de IPS: Análise de decodificação de protocolo;

7.5.14. Deverá possuir o seguinte mecanismos de inspeção de IPS: Análise para detecção de anomalias de protocolo;

7.5.15. Deverá possuir o seguinte mecanismos de inspeção de IPS: Análise heurística;

7.5.16. Deverá possuir o seguinte mecanismos de inspeção de IPS: IP Defragmentation;

7.5.17. Deverá possuir o seguinte mecanismos de inspeção de IPS: Remontagem de pacotes de TCP;

7.5.18. Deverá possuir o seguinte mecanismos de inspeção de IPS: Bloqueio de pacotes malformados;

7.5.19. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc.;

7.5.20. Detectar e bloquear a origem de portscans;

7.5.21. Bloquear ataques efetuados por worms conhecidos;

7.5.22. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;

7.5.23. Possuir assinaturas para bloqueio de ataques de buffer overflow;

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

7.5.25. Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações;

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

7.5.27. Identificar e bloquear comunicação com botnets;

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

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

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

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

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

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

7.5.34. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;

7.5.35. Deve ser possível a configuração de diferentes políticas de controle de

ameaças e ataques baseado em políticas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc., ou seja, cada política de firewall poderá ter uma configuração diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.

7.6. FILTRO DE URL

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

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

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

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

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

7.6.6. Possuir pelo menos 60 categorias de URLs;

7.6.7. Deve possuir a função de exclusão de URLs do bloqueio, por categoria;

7.6.8. Permitir a customização de página de bloqueio;

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

7.7. IDENTIFICAÇÃO DE USUÁRIOS

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

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

7.7.3. Deve possuir integração e suporte a Microsoft Active Directory para os seguintes sistemas operacionais: Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 e Windows Server 2012 R2;

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

usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários ou qualquer tipo de restrição de uso como, mas não limitado à utilização de sistemas virtuais, segmentos de rede, etc.;

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

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

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

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

7.7.9. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;

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

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

7.8. QoS E TRAFFIC SHAPING

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

7.8.2. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem;

7.8.3. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de destino;

7.8.4. Suportar a criação de políticas de QoS e Traffic Shaping por usuário e grupo;

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

7.8.6. Suportar a criação de políticas de QoS e Traffic Shaping por porta;

7.8.7. O QoS deve possibilitar a definição de tráfego com banda garantida;

7.8.8. O QoS deve possibilitar a definição de tráfego com banda máxima;

7.8.9. O QoS deve possibilitar a definição de fila de prioridade;

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

7.8.11. Suportar marcação de pacotes Diffserv, inclusive por aplicação;

7.8.12. Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping;

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

7.9. FILTRO DE DADOS

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

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

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

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

7.10. GEO LOCALIZAÇÃO

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

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

7.11. VPN

7.11.1. Suportar VPN Site-to-Site e Cliente-To-Site;

7.11.2. Suportar IPSec VPN;

7.11.3. Suportar SSL VPN;

7.11.4. A VPN IPSEc deve suportar 3DES;

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

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

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

7.11.8. A VPN IPSEc deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);

7.11.9. A VPN IPSEc deve suportar Autenticação via certificado IKE PKI

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

7.11.11. Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de throubleshooting;

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

7.11.13. A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;

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

7.11.15. Atribuição de DNS nos clientes remotos de VPN;

7.11.16. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Anti-spyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;

7.11.17. Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local;

7.11.18. Suportar leitura e verificação de CRL (certificate revocation list);

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

7.11.20. Deve permitir que a conexão com a VPN seja estabelecida das seguintes forma: Antes do usuário autenticar na estação;

7.11.21. Deve permitir que a conexão com a VPN seja estabelecida das seguintes forma: Após autenticação do usuário na estação;

7.11.22. Deve permitir que a conexão com a VPN seja estabelecida das seguintes forma: Sob demanda do usuário;

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

7.11.24. O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bits), Windows 8 (32 e 64 bits), Windows 10 (32 e 64 bits) e Mac OS X (v10.10 ou superior).

7.12. REQUISITOS MÍNIMOS SOLUÇÃO DE NGFW – FIREWALL DE PRÓXIMA GERAÇÃO

7.12.1. A plataforma de segurança deve possuir a capacidade e as características abaixo, por equipamento:

7.12.1.1. Throughput de, no mínimo, 35 Gbps com a funcionalidade de firewall e controle de aplicação habilitada para tráfego IPv4 e IPv6, independentemente do tamanho do pacote;

7.12.1.2. Throughput de controle de aplicação de 27 Gbps com tráfego HTTP, 64 Kbytes;

7.12.1.3. Suporte a, no mínimo, 8M conexões simultâneas;

7.12.1.4. Suporte a, no mínimo, 200 novas conexões por segundo;

7.12.1.5. Throughput de, no mínimo, 5 Gbps de VPN IPSec e VPN SSL;

7.12.1.6. Estar licenciado para, ou suportar sem o uso de licença, 10000 túneis de VPN IPSEC Site-to-Site simultâneos;

7.12.1.7. Estar licenciado para, ou suportar sem o uso de licença, 15000 túneis de clientes VPN IPSEC simultâneos;

7.12.1.8. Estar licenciada para ou suportar sem uso de licença, 14000 clientes de VPN SSL simultâneos;

7.12.1.9. Suportar no mínimo 20 Gbps de throughput de IPS;

7.12.1.10. Suportar no mínimo 15 Gbps de throughput de Inspeção SSL;

7.12.1.11. Throughput de, no mínimo, 15 Gbps com as seguintes funcionalidade habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS, Antivírus e Antispyware.

7.12.1.12. Possuir ao menos 1 interfaces 1Gbps para gerenciamento;

7.12.1.13. Possuir ao menos 16 interfaces 10Gbps;

7.12.1.14. Disco de, no mínimo, 480 GBytes para armazenamento de informações locais

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

7.12.1.16. Suporte a, no mínimo, 20 sistemas virtuais lógicos (Contextos) por appliance;

7.12.1.17. Deverá acompanhar pelo menos 10 adaptadores Gbics 10Gbps do tipo SR por equipamento;

7.12.1.18. Fonte 120/240 AC ou DC, conforme disponível no local de instalação, redundante e hot-swappble;

7.13. <u>CONSOLE DE GERÊNCIA E MONITORAÇÃO</u>

7.13.1. Deve suportar receber logs de, no mínimo, 2K dispositivos;

7.13.2. Suportar, no mínimo, 7500 logs/segundo de forma contínua;

7.13.3. Permitir acesso simultâneo de administradores permitindo a criação de ao menos 2 (dois) perfis para administração e monitoração;

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

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

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

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

7.13.8. Autenticação integrada a servidor Radius;

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

7.13.10. Geração de relatórios em tempo real, para a visualização de tráfego observado;

7.13.11. Autenticação integrada ao Microsoft Active Directory;

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

7.13.13. Deve possuir um assistente para adicionar dispositivos via interface gráfica usando o IP, login e senha dos mesmos;

7.13.14. Deve ser possível visualizar a quantidade de logs enviado de cada dispositivo monitorado;

7.13.15. Possuir mecanismo para que logs antigos sejam removidos automaticamente;

7.13.16. Permitir a importação e exportação de relatórios;

7.13.17. Deve possuir a capacidade de criar relatórios nos formatos HTML;

7.13.18. Deve possuir a capacidade de criar relatórios nos formatos PDF;

7.13.19. Deve possuir a capacidade de criar relatórios nos formatos XML

7.13.20. Deve possuir a capacidade de criar relatórios nos formatos CSV;

7.13.21. Deve ser possível exportar os logs em CSV;

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

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

7.13.24. A solução deve possuir relatórios pré-definidos;

7.13.25. Possuir envio automático de logs para um servidor FTP externo a solução;

7.13.26. Possibilitar a duplicação de relatórios existentes e edita-los logo após;

7.13.27. Possuir a capacidade de personalização de capas para os relatórios;

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

7.13.29. Logs de auditoria para configurações de regras e objetos devem ser

visualizados em uma lista diferente da que exibe os logs relacionados a tráfego de dados;

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

7.13.31. Deve possuir mecanismo "Drill-Down" para navegação nos relatórios em tempo real;

7.13.32. Dever ser possível fazer download dos arquivos de logs recebidos;

7.13.33. Deve possuir agendamento para gerar e enviar automaticamente relatórios;

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

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

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

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

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

7.13.39. Deve ser possível definir filtros nos relatórios;

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

7.13.41. Permitir que relatórios criado sejam no idioma Português;

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

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

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

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

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

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

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

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

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

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

7.13.52. Deve permitir ver em tempo real os logs recebidos;

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

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

7.13.55. Deve possuir relatório de PCI DSS Compliance;

7.13.56. Deve possuir relatório de utilização de aplicações SAAS;

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

7.13.58. Deve possuir relatório de VPN;

7.13.59. Deve possuir relatório de Sistemas de prevenção de intrusão (IPS);

7.13.60. Deve possuir relatório de reputação do cliente;

7.13.61. Deve possuir relatório de análise de segurança do usuário;

7.13.62. Deve possuir relatório de avaliação da ameaça cibernética;

7.13.63. Deve possuir relatório de equipamentos terminais de solução de segurança gerenciada;

7.13.64. Deve possuir relatório de análise de segurança e uso de web, se há uma plataforma de cache;

7.13.65. Deve possuir relatório de análise aplicações web, se há uma plataforma de segurança web.

8. MODELO DE PLANILHA DE ATENDIMENTO A REQUISITOS

8.4. O atendimento a todos os itens deve ser comprovado através de documentação oficial do fabricante da solução, que deverá ser anexada à proposta comercial ajustada. A instituição poderá realizar diligência junto ao fabricante para comprovar a autenticidade da documentação. A localização da comprovação na(s) página(s) deverá ser clara e precisa. O não atendimento destes requisitos implicará na desclassificação da proposta.

Item	Documento	Página	Localização

DOS SERVIÇOS DE MANUTENÇÃO E ASSISTÊNCIA TÉCNICA

8.5. O período de prestação de serviços de manutenção e assistência técnica deverá ser de 36 (trinta e seis) meses, contado a partir da data de assinatura do contrato;

8.6. Forma de Atendimento da Assistência Técnica:

8.6.1. A Contratada deverá disponibilizar "Central de Atendimento" para abertura de chamado de assistência técnica, em dias úteis (segunda-feira à sexta-feira), em horário comercial (08h às 18h), indicando telefone 0800, ou número local em Fortaleza-CE. Os chamados poderão ser abertos pela equipe técnica da contratante.

8.6.2. O atendimento será do tipo on-site (no local) mediante manutenção corretiva na localidade de entrega dos itens deste Termo de Referência, incluindo serviços e peças, com janela de atendimento de 24x7, 24 (Vinte e Quatro) horas (00h às 23h59min) e 07 (Sete) dias por semana (Segunda à Segunda), com Tempo de Solução de até 48 (quarenta e oito) horas. O atendimento deverá ser realizado por profissionais especializados e deverá cobrir todo e qualquer defeito apresentado, incluindo o fornecimento e a substituição de peças e/ou componentes, ajustes, reparos e correções necessárias;

8.6.3. A substituição de peças e/ou componentes mecânicos ou eletrônicos de marcas e/ou modelos diferentes dos originais cotados pela contratada, desde que o fabricante assegure que não haverá perda da garantia, somente poderá ser efetuada mediante análise e autorização da contratante.

8.6.4. Todas as peças e componentes mecânicos ou eletrônicos substitutos deverão apresentar padrões de qualidade e desempenho iguais ou superiores aos utilizados na fabricação do(s) equipamento(s), sempre "novos e de primeiro uso", não podendo ser recondicionados.

9. DOS RECURSOS ORÇAMENTÁRIOS

10.1. As despesas decorrentes desta licitação correrão à conta de dotações consignadas abaixo:

Projeto Atividade: 04.126.0106.1062.0001, Elementos de Despesa: 44.90.39 e 44.9052, Fontes de Recurso: 30101 e 33101, do orçamento da Secretaria Municipal do Planejamento, Orçamento e Gestão – SEPOG.

11. DA ENTREGA E DO RECEBIMENTO

11.1. Quanto à entrega:

11.1.1. O objeto contratual deverá ser entregue em conformidade com as especificações estabelecidas neste instrumento, nos locais indicados pela Coordenadoria de Gestão Corporativa de Tecnologia da Informação da Secretaria Municipal do Planejamento, Orçamento e Gestão.

11.1.2. O prazo de entrega do objeto a ser adquirido pelo órgão contratante será de **até 30 (trinta) dias,** contados do recebimento pela empresa da ordem de fornecimento/serviço.

11.1.3**.** Os atrasos ocasionados por motivo de força maior ou caso fortuito, desde que justificados até 2 (dois) dias úteis antes do término do prazo de entrega, e aceitos pela contratante, não serão considerados como inadimplemento contratual.

11.1.4**.** A responsabilidade administrativa pelo recebimento do objeto tal qual estipulado no edital será exclusiva da servidor/Comissão de Fiscalização designada pelo órgão participante, encarregada de acompanhar a execução do processo de entrega e recebimento dos objetos do contrato, conforme art. 67 da Lei 8.666/93.

11.1.5. Os equipamentos deverão ser entregues rigorosamente de acordo com as especificações estabelecidas no Anexo A – Termo de Referência deste edital, bem como na proposta vencedora, sendo que a não observância destas condições, implicará na não aceitação do mesmo, sem que caiba qualquer tipo de reclamação ou indenização por parte da inadimplente.

11.1.6**.** A CONTRATANTE designará um servidor/comissão, cujo propósito será o acompanhamento da entrega e a conferência desta com as especificações contidas na proposta de preços e no Termo de Referência. Caso o objeto esteja em desacordo com as especificações contidas naqueles instrumentos, será rejeitado o recebimento do mesmo.

11.1.7. Devem ser entregues juntamente com os equipamentos, a documentação técnica (impressa ou em CD), incluindo manuais de configuração, CDs, DVDs.

11.2. Quanto ao recebimento:

11.2.1. **PROVISORIAMENTE**, até 10 (dez) dias da entrega do produto, mediante Termo de Recebimento Provisório, para efeito de posterior verificação da conformidade do objeto com as especificações, devendo ser feito pelo(s) fiscal(is) do contrato.

11.2.2**. DEFINITIVAMENTE**, até 30 (trinta) dias da expedição do termo de recebimento provisório, após a verificação da qualidade e da quantidade do objeto, certificando-se de que todas as condições estabelecidas foram atendidas e, consequente aceitação das notas fiscais pelo(s) fiscal(is) da contratação, será expedido termo de recebimento definitivo, devendo haver rejeição do objeto no caso de desconformidade. O Termo de recebimento definitivo será lavrado pelo(s) fiscal(is) do contrato.

11.2.2.1 A nota fiscal/fatura que apresente incorreções será devolvida à contratada para as devidas correções, no prazo estabelecido pela Administração. Nesse caso, o termo de recebimento definitivo somente poderá ser emitido após a referida correção.

11.2.3. O recebimento dos produtos, em caráter provisório ou definitivo, será realizado de segunda a sexta-feira, no horário de 8h às 12h. e de 13h ás 17h

11.2.4. A Administração rejeitará, no todo ou em parte, a entrega dos bens em desacordo com as especificações técnicas exigidas.

11.2.5. Em caso de troca do objeto a mesma deverá ser efetuada no endereço do órgão contratante.

11.2.6. O Contratado deverá providenciar a troca do objeto no prazo máximo de 2 (dois) dias do registro da ocorrência.

11.2.7. A rejeição do objeto por estar em desacordo com as especificações, que vier a ocorrer, não justificará possível atraso no prazo de entrega fixado, sujeitando o licitante vencedor às sanções previstas.

12. DO PAGAMENTO

12.1. O pagamento será efetuado mensalmente após a emissão da nota de empenho e será no prazo máximo de 30 (trinta) dias contados a partir da lavratura do Termo de Recebimento Definitivo da parcela executada, mediante crédito em conta corrente em nome da contratada, no Banco do Brasil S/A.
12.2. Não será efetuado qualquer pagamento à contratada, em caso de descumprimento do objeto, conforme especificações exigidas na licitação.
12.3. É vedada a realização de pagamento antes da execução do objeto ou se o mesmo não estiver de acordo com as especificações deste instrumento.
12.4. Os pagamentos encontram-se ainda condicionados à apresentação dos seguintes comprovantes:
12.4.1. Documentação relativa à regularidade para com as Fazendas Federal, Estadual e Municipal, o Fundo de Garantia por Tempo de Serviço (FGTS) e a Justiça Trabalhista.
12.5. Toda a documentação exigida deverá ser apresentada em original ou por qualquer processo de reprografia, obrigatoriamente autenticada em cartório. Caso esta documentação tenha sido emitida pela Internet, só será aceita após a confirmação de sua autenticidade.

12.6. A atualização financeira dos valores a serem pagos, em virtude de inadimplemento pela contratante, será efetuada através do INPC (Índice Nacional de Preços ao Consumidor), *pro rata*, desde a data final do período do adimplemento até a data do efetivo pagamento, desde que comprove que o contratante é o único responsável pelo atraso.

13. DAS SANÇÕES ADMINISTRATIVAS

13.1. O contratado que praticar ato ilícito estará sujeito, garantido o direito prévio de citação e da ampla defesa, sem prejuízo das sanções legais nas esferas civis e criminais, às seguintes penalidades, de acordo com o Decreto Municipal nº 13.735/2016:

I. Advertência, que consista em comunicação formal ao infrator, decorrente da inexecução de deveres que ocasionem riscos e/ou prejuízos de menor potencial ofensivo para a Administração;

II. Multa cumulativa com as demais sanções, conforme estabelecido nos artigos 50 e 51 do Decreto Municipal nº 13.375/2016

III. Impedimento de licitar e contratar com a Administração Direta e Indireta do Município de Fortaleza e descredenciamento no Cadastro de Fornecedores da Central de Licitações da Prefeitura de Fortaleza - CLFOR, pelo prazo de até 05 (cinco) anos.

13.1.1. Entende-se por ato ilícito qualquer conduta comissiva ou omissiva que infrinja dispositivos legais ou regras constantes de regulamentos ou de qualquer outro ato normativo, inclusive aquelas constantes dos atos convocatórios de licitação, da ata de registro de preços, do contrato ou instrumento que o substitua.

13.1.2. A aplicação das multas de natureza moratória não impede a aplicação superveniente de outras multas previstas neste item, cumulando-se os respectivos valores.

13.1.3. O atraso, para efeito de cálculo da multa, será contado em dias corridos, a partir do primeiro dia útil subsequente ao do encerramento do prazo estabelecido para o cumprimento da obrigação

13.1.4. No caso de prestações continuadas, a multa de 5% (cinco por cento) de que trata a alínea “d” deste item será calculada sobre o valor da parcela que eventualmente for descumprida.

13.1.5. A critério da autoridade competente, o valor da multa poderá ser descontado do pagamento a ser efetuado ao contratado, inclusive antes da execução da garantia contratual, quando esta não for prestada sob a forma de caução em dinheiro.

13.1.6. Caso o valor a ser pago ao contratado seja insuficiente para satisfação da multa, a diferença será descontada da garantia contratual.

13.1.7. Caso a faculdade prevista no subitem 13.1.5. não tenha sido exercida e verificada a insuficiência da garantia para satisfação integral da multa, o saldo remanescente será descontado de pagamentos devidos ao contratado.

13.1.8. Caso o valor da garantia seja utilizado, no todo ou em parte, para o pagamento da multa, esta deve ser complementada pelo contratado no prazo de até 10 (dez) dias uteis, a contar da solicitação do contratante.

13.1.9. Após esgotados os meios de execução direta da sanção de multa, o licitante será notificado para recolher a importância devida no prazo de 15 (quinze) dias, contados do recebimento da comunicação oficial. Decorrido o prazo, a CLFOR encaminhará a multa para que seja inscrita na Dívida Ativa do Município.

13.2. Na aplicação das sanções devem ser consideradas as seguintes circunstancias:

I. a natureza e a gravidade da infração cometida;

II. os danos que o cometimento da infração ocasionar aos serviços e aos usuários;

III. a vantagem auferida em virtude da infração;

IV. as circunstancias gerais agravantes e atenuantes;

V. os antecedentes da licitante ou contratada.

14. DAS OBRIGAÇÕES DA CONTRATADA

14.1. Executar o objeto em conformidade com as condições deste instrumento.

14.2. Manter durante toda a execução contratual, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação.

14.3. Aceitar, nas mesmas condições contratuais, os percentuais de acréscimos ou supressões limitados ao estabelecido no §1º, do art. 65, da Lei Federal nº 8.666/1993, tomando-se por base o valor contratual.

14.4. Responsabilizar-se pelos danos causados diretamente à contratante ou a terceiros, decorrentes da sua culpa ou dolo, quando da execução do objeto, não podendo ser arguido para efeito de exclusão ou redução de sua responsabilidade o fato de a contratante proceder à fiscalização ou acompanhar a execução contratual.

14.5. Responder por todas as despesas diretas e indiretas que incidam ou venham a incidir sobre a execução contratual, inclusive as obrigações relativas a salários, previdência social, impostos, encargos sociais e outras providências, respondendo obrigatoriamente pelo fiel cumprimento das leis trabalhistas e específicas de acidentes do trabalho e legislação correlata, aplicáveis ao pessoal empregado na execução contratual.

14.6. Responder por todos os prejuízos, perdas e danos que venham a ocorrer referentes ao transporte e entrega dos produtos.

14.7. Prestar imediatamente as informações e os esclarecimentos que venham a ser solicitados pela contratante, salvo quando implicarem em indagações de caráter técnico, hipótese em que serão respondidas no prazo de 24 (vinte e quatro) horas.

14.8. Substituir ou reparar o objeto contratual que comprovadamente apresente condições de defeito ou em desconformidade com as especificações deste termo, no prazo máximo de 2 (dois) dias do registro da ocorrência.

14.9. Caso o material, objeto da troca do item anterior, também apresente defeito, o dever de substituí-lo é no prazo máximo de **2 (dois) dias.**

14.10. Cumprir, quando for o caso, as condições de garantia do objeto, responsabilizando-se pelo período oferecido em sua proposta de preços, observando o prazo mínimo exigido pela Administração.

14.11. Os produtos deverão vir lacrados de forma a proteger da ação da luz, poeira umidade, sendo que, nos casos das embalagens apresentarem violação de qualquer espécie, deverão ser substituídas pelo fornecedor, ainda que na fase de análise/recebimento.

14.12. Providenciar a substituição de qualquer empregado que esteja a serviço da contratante, cuja conduta seja considerada indesejável pela fiscalização da contratante.

14.13. Entregar os materiais em conformidade com o presente Termo de Referência e com a proposta em **até 30 (trinta) dias,** contados do recebimento pela empresa da ordem de fornecimento/serviço.

14.14. Discriminar na nota fiscal as especificações do material de modo idêntico àquele apresentado na proposta.

14.15. Não transferir a outrem, por qualquer forma, nem mesmo parcialmente, em subcontratar, qualquer das prestações a que está obrigada por força deste Termo de Referência e seus anexos.

14.16. Assegurar a garantia estipulada, não inferior a 12 (doze) meses, contra defeitos de fabricação, independente de ser ou não o fabricante, devendo providenciar a correção ou a substituição de todos os materiais adquiridos que apresentarem defeitos ou divergência com as especificações fornecidas.

14.17. Arcar com todas as despesas decorrentes do fornecimento dos equipamentos nos locais indicados, e, ainda, com todos os encargos diretos e indiretos que incidir sobre a comercialização dos materiais e seus elementos suplementares e eventuais substituições/ reposições.

14.18. Ressarcir qualquer dano ou prejuízo causado à contratante e/ou a terceiros, provocados por ação ou omissão, ineficiência ou irregularidade cometidas por seus empregados, convenentes, envolvidos na execução do contrato, bem como, assumir inteira responsabilidade civil, administrativa e penal por qualquer prejuízo, material ou pessoal, causados à contratante ou a terceiros.

14.19. Aceitar, sem restrições, a fiscalização da Contratante, no que diz respeito ao fiel cumprimento das condições de fornecimento dos equipamentos.

14.20. Manter-se, durante todo o período de vigência da Ata / Contrato a ser firmado, um preposto aceito pela Contratante, para representação do licitante vencedor sempre que for necessário e comunicando, por escrito, à Contratante qualquer mudança de endereço ou telefone contato.

14.21. Acatar as orientações da Contratante, sujeitando-se a mais ampla e irrestrita fiscalização, prestando os esclarecimentos solicitados e atendendo às reclamações formuladas.

15. DAS OBRIGAÇÕES DA CONTRATANTE

15.1. Solicitar a execução do objeto à CONTRATADA através da emissão de Ordem de Fornecimento/Serviço, após emissão de empenho.

15.2. Proporcionar à CONTRATADA todas as condições necessárias ao pleno cumprimento das obrigações decorrentes do objeto contratual, consoante estabelece a Lei Federal no 8.666/1993 e suas alterações posteriores.

15.3. Fiscalizar a execução do objeto contratual, através de sua unidade competente, podendo, em decorrência, solicitar providências da CONTRATADA, que atenderá ou justificará de imediato.

15.4. Notificar a CONTRATADA de qualquer irregularidade decorrente da execução do objeto contratual.

15.5. Efetuar os pagamentos devidos à CONTRATADA nas condições estabelecidas neste Termo.

15.6. Aplicar as penalidades previstas em lei e neste instrumento.

15.7. Receber os materiais entregues pela contratada que estejam em conformidade com a proposta aceita.

15.8. Recusar, com a devida justificativa, qualquer material entregue fora das especificações constantes neste Termo de Referência.

15.9. Fornecer, mediante solicitação escrita da contratada, informações adicionais, dirimir dúvidas e orientá-la nos casos omissos.

16. MEDIDAS ACAUTELADORAS

16.1. Consoante o art. 45, da Lei 9.784/1999, a Administração Pública poderá, sem a prévia manifestação do interessado, motivadamente, adotar providências acauteladoras, em caso de risco iminente, como forma de prevenir a ocorrência de dano de difícil ou impossível reparação.

17. CONTROLE DA EXECUÇÃO

17.1. A fiscalização da contratação será exercida por um(a) servidor/comissão nomeado(a) pela Contratante, ao qual competirá dirimir as dúvidas que surgirem no curso da execução do objeto e de tudo dar ciência à Administração, de acordo com o estabelecido no art. 67, da Lei Federal nº 8.666/1993, a ser informado e designado para este fim pela contratante, quando da lavratura do instrumento contratual.

17.2. A fiscalização de que trata este item não exclui nem reduz a responsabilidade do Contratado, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, ou emprego de material inadequado ou de qualidade inferior, e, na ocorrência desta, não implica em corresponsabilidade dos órgãos ou de seus agentes e prepostos, de conformidade com o art. 70, da Lei 8.666/1993.

18. AVALIAÇÃO DO CUSTO

18.1. O custo total estimado da licitação é de R$ 1.915.176,85 (hum milhão, novecentos e quinze mil, cento e setenta e seis reais e oitenta e cinco centavos).

18.2. O custo estimado foi apurado a partir de mapa de preços constante do processo administrativo elaborado com base em orçamentos recebidos de empresas pertencentes ao ramo do objeto licitado. O referido Mapa de Preços,foi elaborado, a partir dos custos unitários de cada lote.

19. PRAZO DE VIGÊNCIA E DE EXECUÇÃO DO CONTRATO

19.1. O prazo de vigência contratual é de 12 (doze) meses, contados a partir da sua assinatura, devendo ser publicado na forma do parágrafo único do art. 61 da Lei Federal nº 8.666/1993.

19.2. O prazo de execução contratual se iniciará a partir do recebimento da Ordem de Fornecimento/Serviço, após a emissão do empenho.

19.3. Os prazos de vigência e de execução deste contrato poderão ser prorrogados nos termos do que dispõe o art. 57, da Lei Federal n° 8.666/1993.

ANEXO B – MODELO DA PROPOSTA DE PREÇOS

(Papel timbrado ou personalizado do licitante)

PROPOSTA DE PREÇOS

(O modelo desta proposta de preços visa facilitar a análise comparativa entre as mesmas)

À

Central de Licitações da Prefeitura de Fortaleza

Att. Sr. Pregoeiro

Ref.: Pregão Eletrônico nº _____

A Empresa _____ sediada à (rua, bairro, cidade, telefone, etc.), nº ___, inscrita no CNPJ/MF sob nº _____, neste ato representado por _____ (nome e dados do representante legal), abaixo assinado, propõe a entrega dos objetos a seguir especificado, conforme Termo de Referência do Edital em epígrafe, nas seguintes condições:

1. Identificação do licitante:

a. Razão Social:

b. CPF/CNPJ e Inscrição Estadual:

c. Endereço completo:

d. Representante Legal (nome, nacionalidade, estado civil, profissão, RG, CPF, domicílio):

e. Telefone, celular, fax, e-mail:

f. Banco do Brasil S/A, agência e nº da conta corrente:

2. Condições Gerais da Proposta:

a. A presente proposta é válida por _____(_____) dias, contados da data de sua emissão. **(Não inferior a 90 (noventa) dias, a contar da data da sua apresentação.)**

3. Formação do Preço por LOTE:

Lote /Item	Especificação	Marca / Fabricante	Unidade	Quantidade	Valor Unitário R$	Valor Total do Item R$
VALOR TOTAL DO LOTE:						

(A especificação de cada item deverá estar detalhada conforme Item 06 do Termo de Referência.)

VALOR GLOBAL

Valor por extenso (_____)

1. Declaramos que o objeto cotado atende todas as exigências do edital, relativas à especificação e características, inclusive técnicas e que estamos de pleno acordo com todas as condições estabelecidas no edital e seus anexos.

2. Nos preços estão inclusos todos os custos diretos e indiretos, lucro, encargos trabalhistas e despesas com seguros, frete, mão-de-obra e outras necessárias ao cumprimento integral do objeto deste Pregão e excluídos da composição dos preços ofertados o imposto de renda pessoa jurídica (IRPF) e a contribuição social sobre o lucro líquido (CSLL).

3. O prazo de entrega do objeto será de (observar o limite máximo do Termo de Referência).

4. O local de entrega do objeto será o indicado no Termo de Referência.

5. Caso nos seja adjudicado o objeto da presente licitação, nos comprometemos assinar o contrato e a receber as ordens de fornecimento / serviço, nota de empenho no prazo previsto no ato de convocação, indicando para esse fim o Sr. _____, identidade nº _____, CPF nº _____, _____ (cargo), como responsável legal desta empresa.

6. Declaramos que estamos cientes que a validade do contrato será de 12 (doze) meses, contados da data de sua assinatura.

Local e data

Assinatura do representante legal

(Nome e cargo)

ANEXO C – DECLARAÇÃO DE MICROEMPRESA, EMPRESA DE PEQUENO PORTE OU COOPERATIVA *(modelo meramente sugestivo)*

(PAPEL TIMBRADO DO PROPONENTE)

(nome /razão social) _____, inscrita no CNPJ nº_____,por intermédio de seu representante legal o(a) Sr(a)_____, portador(a) da Carteira de Identidade nº_____e CPF nº _____, DECLARA, sob as sanções administrativas cabíveis e sob as penas da lei, ser _____(microempresa, empresa de pequeno porte ou cooperativa) nos termos da legislação vigente, não possuindo nenhum dos impedimentos previstos no § 4º, do art. 3º, da Lei Complementar nº 123/2006.

Local e data

Assinatura do representante legal
(Nome e cargo)

ANEXO D – MODELO DE DECLARAÇÃO

DECLARAÇÃO DE CONTRATOS FIRMADOS COM A INICIATIVA PRIVADA E ADMINISTRAÇÃO PÚBLICA

Declaramos que a empresa _____, inscrita no CNPJ (MF) nº _____, inscrição estadual nº _____, estabelecida no (a) _____ que possui os seguintes contratos firmados com a iniciativa privada e administração pública:

Nome do Órgão/Empresa	Nº/Ano do Contrato	Valor total do Contrato
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

Valor total dos Contratos _____

Local e data

_____
Assinatura e carimbo do emissor

Observação: 1) O licitante deverá informar todos os contratos vigentes.

ANEXO E - MINUTA DO CONTRATO

Contrato nº ___ / ____ – (Órgão Contratante)

Processo nº **P661335/2017**

CONTRATO QUE ENTRE SI CELEBRAM (O)A _____ _____ E (O) A _____, ABAIXO QUALIFICADOS, PARA O FIM QUE NELE SE DECLARA.

A(O) _____ situada(o) na _____, inscrita(o) no CNPJ sob o nº _____, doravante denominada(o) CONTRATANTE, neste ato representada(o) pelo _____, (nacionalidade), portador da Carteira de Identidade nº _____, e do CPF nº _____, residente e domiciliada(o) em (Município - UF), na _____, e a _____, com sede na _____, CEP: _____, Fone: _____, inscrita no CPF/CNPJ sob o nº _____, doravante denominada CONTRATADA, representada neste ato pelo _____, (nacionalidade), portador da Carteira de Identidade nº _____, e do CPF nº _____, residente e domiciliada(o) em (Município - UF), na _____, têm entre si justa e acordada a celebração do presente contrato, mediante as cláusulas e condições seguintes:

CLÁUSULA PRIMEIRA – DA FUNDAMENTAÇÃO

1.1. O presente contrato tem como fundamento o edital do **Pregão Eletrônico n°.** ____**/**____ e seus anexos, o que consta nos autos do processo administrativo **nº. P661335/2017,** os preceitos do direito público, Lei Federal nº. 10.520, de 17 de Julho de 2002 e a Lei Federal nº. 8.666/1993 e suas alterações posteriores e outras leis especiais necessárias ao cumprimento de seu objeto.

CLÁUSULA SEGUNDA – DA VINCULAÇÃO AO EDITAL E A PROPOSTA

2.1. O cumprimento deste contrato está vinculado aos termos do edital do **Pregão Eletrônico n°.** ____**/**____ e seus anexos e à proposta da CONTRATADA, os quais constituem parte deste instrumento, independente de sua transcrição.

CLÁUSULA TERCEIRA – DO OBJETO

3.1. CONTRATAÇÃO DE EMPRESA ESPECIALIZADA NO FORNECIMENTO DE SOLUÇÃO INTEGRADA DE SEGURANÇA DE PERÍMETRO (FIREWALL), QUE POSSIBILITE A VISIBILIDADE E CONTROLE DE TRÁFEGO, FILTRAGEM DE CONTEÚDO WEB, PREVENÇÃO CONTRA AMEAÇAS DE REDES MODERNAS, FILTRO DE DADOS, VPN E CONTROLE GRANULAR DE BANDA DE REDE, COMPREENDENDO FORNECIMENTO DE EQUIPAMENTOS

E SOFTWARES INTEGRADOS, *APPLIANCE*, LICENCIAMENTO E GARANTIA DE ATUALIZAÇÃO PARA ATENDER AS NECESSIDADES DA PREFEITURA MUNICIPAL DE FORTALEZA, DE ACORDO COM AS ESPECIFICAÇÕES E QUANTITATIVOS CONTIDOS NO ANEXO A – TERMO DE REFERÊNCIA DO EDTIAL PREGÃO ELETRÔNICO _____/2017, PARA O PERÍODO DE 12 MESES.

3.2. Dos LOTES contratados:

LOTE/ ITEM	DESCRIÇÃO	UND.	QTD.	MARCA/ FABRICANTE	VALOR UNITÁRIO (R$)	VALOR TOTAL (R$)

3.3. DETALHAMENTO DAS ESPECIFICAÇÕES TÉCNICAS MÍNIMAS - CARACTERÍSTICAS GERAIS

3.3.1 Prover solução de segurança perimetral que inclui Firewall de Próxima Geração com Controle de Ameaças Avançadas, com desempenho suficiente para suportar a ativação e configuração simultânea de todas as funcionalidades e recursos descritos neste termo para os valores de desempenho descritos;

3.3.2 As funcionalidades de segurança descritas nesta especificação devem ser disponibilizadas em hardware do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;

3.3.3 As funcionalidades de proteção de rede que compõe a plataforma de segurança devem funcionar no mesmo appliance, não sendo aceito soluções onde aja a necessidade da combinação de múltiplos dispositivos para composição da solução de segurança ofertada;

3.3.4 Todo o ambiente deverá ser gerenciado através de uma única interface do próprio fabricante da solução, sem a necessidade de produtos de terceiros para compor a solução;

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

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

3.3.7 A gerência poderá ser virtualizada, desde que compatível com as plataformas de virtualização da VMware e/ou Hyper-V e/ou RHEV, ou fornecida em hardware do tipo appliance;

3.3.8 Todos os equipamentos físicos (hardware) fornecidos devem ser próprios para montagem em rack 19”, incluindo kit tipo trilho para adaptação, se necessário, e cabos de alimentação;

3.3.9 O software da solução de segurança deverá ser fornecido em sua versão mais atual e estável possível, até a data de publicação deste certame, não sendo permitido qualquer tipo de comprovação futura e/ou versões que não estejam publicadas em sua versão final

no site do próprio fabricante, não sendo aceitos também versões experimentais, versões de teste e/ou customizadas para clientes específicos;

3.3.10 A solução de segurança deve incluir todas as licenças necessárias para o perfeito funcionamento de todas as funcionalidades descritas nesta especificação por 03 (três) anos, incluindo a atualização de sua base de assinaturas;

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

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

3.4. REQUISITOS MÍNIMOS

3.4.1 Suporte a 4094 VLAN Tags 802.1q;

3.4.2 Agregação de links 802.3ad e LACP;

3.4.3 Policy based routing ou policy based forwarding;

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

3.4.5 Suporte a DHCP Relay;

3.4.6 Suporte a DHCP Server;

3.4.7 Suporte a Jumbo Frames;

3.4.8 Deve suportar os seguintes tipos de NAT:

3.4.8.1 Deve suportar NAT dinâmico (Many-to-1);

3.4.8.2 Deve suportar NAT dinâmico (Many-to-Many);

3.4.8.3 Deve suportar NAT estático (1-to-1);

3.4.8.4 Deve suportar NAT estático (Many-to-Many);

3.4.8.5 Deve suportar NAT estático bidirecional 1-to-1;

3.4.8.6 Deve suportar Tradução de porta (PAT);

3.4.8.7 Deve suportar NAT de Origem;

3.4.8.8 Deve suportar NAT de Destino;

3.4.8.9 Deve suportar NAT de Origem e NAT de Destino simultaneamente;

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

3.4.8.11 Deve suportar NAT64 e NAT46;

3.4.8.12 Deve implementar o protocolo ECMP;

3.4.8.13 Deve implementar balanceamento de link por hash do IP de origem;

3.4.8.14 Deve implementar balanceamento de link por hash do IP de origem e destino;

3.4.8.15 Deve implementar balanceamento de link por hash do IP de origem;

3.4.8.16 Deve implementar balanceamento de link por hash do IP de origem e destino;

3.4.8.17 Deve implementar balanceamento de link através do método round-robin;

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

3.4.8.19 Deve implementar balanceamento de link através de políticas por usuário e grupos de usuários do LDAP/AD;

3.4.8.20 Deve implementar balanceamento de link através de políticas por aplicação e porta de destino;

3.4.8.21 Deve implementar balanceamento de links sem a necessidade de criação de

zonas ou uso de instâncias virtuais

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

3.4.8.23 Enviar log para sistemas de monitoração externos, simultaneamente;

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

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

3.4.8.26 Proteção contra anti-spoofing;

3.4.8.27 Para IPv4, deve suportar roteamento estático e dinâmico:

3.4.8.27.1 RIPv2;

3.4.8.27.2 BGP;

3.4.8.27.3 OSPFv2.

3.4.8.28 Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);

3.4.8.29 Suportar OSPF graceful restart;

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

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

3.4.8.32 Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;

3.4.8.33 Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha visibilidade do tráfego;

3.4.8.34 Deve suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;

3.4.8.35 Implementar otimização do tráfego entre dois equipamentos;

3.4.8.36 Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo:

3.4.8.36.1 Em modo transparente;

3.4.8.36.2 Em layer 3;

3.4.8.36.3 Em layer 3 e com no mínimo 3 equipamentos no cluster.

3.4.8.37 A configuração em alta disponibilidade deve sincronizar:

3.4.8.37.1 Sessões;

3.4.8.37.2 Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede;

3.4.8.37.3 Associações de Segurança das VPNs;

3.4.8.37.4 Tabelas FIB;

3.4.8.37.5 Certificados de-criptografados;

3.4.8.37.6 Associações de Segurança das VPNs;

3.4.8.38 Os dispositivos de proteção de rede devem suportar subinterfaces ethernet logicas

3.4.8.39 O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link;

3.4.8.40 Deve possuir suporte à criação de sistemas virtuais no mesmo appliance;

3.4.8.41 Em alta disponibilidade, deve ser possível o uso de clusters virtuais, seja ativo-ativo ou ativo-passivo, permitindo a distribuição de carga entre diferentes contextos;

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

3.4.8.43 Controle, inspeção e descriptografia de SSL para tráfego de entrada (Inbound) e Saída (Outbound), sendo que deve suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos).

3.5.REQUISITOS POR FUNCIONALIDADE

3.5.1. CONTROLE POR POLÍTICA DE FIREWALL

3.5.1.1. Deverá suportar controles por zona ou grupo de segurança;

3.5.1.2. Controles de políticas por porta e protocolo;

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

3.5.1.4. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas ou grupo de segurança;

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

3.5.1.6. Deve suportar offload de certificado em inspeção de conexões SSL de entrada (Inbound);

3.5.1.7. Deve descriptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.2;

3.5.1.8. Controle de inspeção e descriptografia de SSH por política;

3.5.1.9. Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada;

3.5.1.10. Traffic shaping QoS baseado em Políticas (Prioridade, Garantia e Máximo);

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

3.5.1.12. Suporte a objetos e regras IPV6;

3.5.1.13. Suporte a objetos e regras multicast;

3.5.1.14. Deve suportar no mínimo três tipos de resposta nas políticas de firewall:

3.5.1.14.1. Drop sem notificação do bloqueio ao usuário;

3.5.1.14.2. Drop com notificação do bloqueio ao usuário;

3.5.1.14.3. Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego, TCP-Reset para o client, TCP-Reset para o server ou para os dois lados da conexão;

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

3.6. CONTROLE DE APLICAÇÕES

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

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

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

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

3.6.5. Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;

3.6.6. Deve detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a bittorrent e aplicações VoIP que utilizam criptografia proprietária;

3.6.7. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede ToR;

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

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

3.6.10. Identificar o uso de táticas evasivas via comunicações criptografadas;

3.6.11. Atualizar a base de assinaturas de aplicações automaticamente;

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

3.6.13. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de

instalação de agente no Domain Controller, nem nas estações dos usuários;

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

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

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

3.6.17. Permitir a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias sem a necessidade de ação do fabricante

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

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

3.6.20. Deve alertar o usuário quando uma aplicação for bloqueada;

3.6.21. Deve possibilitar a diferenciação de tráfegos Peer-to-Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;

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

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

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

3.6.25. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc.)

3.6.26. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Nível de risco da aplicação

3.6.27. Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação

3.7. PREVENÇÃO DE AMEAÇAS AVANÇADAS

3.7.1. Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de Firewall;

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

3.7.3. As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter

permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante;

3.7.4. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;

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

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

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

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

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

3.7.10. Deve permitir o bloqueio de vulnerabilidades

3.7.11. Deve permitir o bloqueio de exploits conhecidos

3.7.12. Deve incluir proteção contra-ataques de negação de serviços

3.7.13. Deverá possuir o seguinte mecanismos de inspeção de IPS: Análise de padrões de estado de conexões;

3.7.14. Deverá possuir o seguinte mecanismos de inspeção de IPS: Análise de decodificação de protocolo;

3.7.15. Deverá possuir o seguinte mecanismos de inspeção de IPS: Análise para detecção de anomalias de protocolo;

3.7.16. Deverá possuir o seguinte mecanismos de inspeção de IPS: Análise heurística;

3.7.17. Deverá possuir o seguinte mecanismos de inspeção de IPS: IP Defragmentation;

3.7.18. Deverá possuir o seguinte mecanismos de inspeção de IPS: Remontagem de pacotes de TCP;

3.7.19. Deverá possuir o seguinte mecanismos de inspeção de IPS: Bloqueio de pacotes malformados

3.7.20. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc.;

3.7.21. Detectar e bloquear a origem de portscans;

3.7.22. Bloquear ataques efetuados por worms conhecidos;

3.7.23. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;

3.7.24. Possuir assinaturas para bloqueio de ataques de buffer overflow;

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

3.7.26. Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações;

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

3.7.28. Identificar e bloquear comunicação com botnets;

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

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

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

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

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

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

3.7.35. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos

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

3.8. FILTRO DE URL

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

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

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

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

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

3.8.6. Possuir pelo menos 60 categorias de URLs;

3.8.7. Deve possuir a função de exclusão de URLs do bloqueio, por categoria;

3.8.8. Permitir a customização de página de bloqueio;

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

3.9. IDENTIFICAÇÃO DE USUÁRIOS

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

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

3.9.3. Deve possuir integração e suporte a Microsoft Active Directory para os seguintes sistemas operacionais: Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 e Windows Server 2012 R2;

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

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

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

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

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

3.9.9. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;

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

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

3.10. QoS E TRAFFIC SHAPING

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

3.10.2. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem;

3.10.3. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de destino;

3.10.4. Suportar a criação de políticas de QoS e Traffic Shaping por usuário e grupo;

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

3.10.6. Suportar a criação de políticas de QoS e Traffic Shaping por porta;

3.10.7. O QoS deve possibilitar a definição de tráfego com banda garantida;

3.10.8. O QoS deve possibilitar a definição de tráfego com banda máxima;

3.10.9. O QoS deve possibilitar a definição de fila de prioridade;

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

3.10.11. Suportar marcação de pacotes Diffserv, inclusive por aplicação;

3.10.12. Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping;

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

3.11. FILTRO DE DADOS

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

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

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

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

3.12. GEO LOCALIZAÇÃO

3.12.1. Suportar a criação de políticas por geo-localização, permitindo o trafego de

determinado Pais/Países sejam bloqueados;

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

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

3.13. VPN

3.13.1. Suportar VPN Site-to-Site e Cliente-To-Site;

3.13.2. Suportar IPSec VPN;

3.13.3. Suportar SSL VPN;

3.13.4. A VPN IPSEc deve suportar 3DES;

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

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

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

3.13.8. A VPN IPSEc deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);

3.13.9. A VPN IPSEc deve suportar Autenticação via certificado IKE PKI

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

3.13.11. Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de throubleshooting;

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

3.13.13. A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;

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

3.13.15. Atribuição de DNS nos clientes remotos de VPN;

3.13.16. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Anti-spyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;

3.13.17. Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local;

3.13.18. Suportar leitura e verificação de CRL (certificate revocation list);

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

3.13.20. Deve permitir que a conexão com a VPN seja estabelecida das seguintes forma: Antes do usuário autenticar na estação;

3.13.21. Deve permitir que a conexão com a VPN seja estabelecida das seguintes forma: Após autenticação do usuário na estação;

3.13.22. Deve permitir que a conexão com a VPN seja estabelecida das seguintes forma: Sob demanda do usuário;

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

3.13.24. O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bits), Windows 8 (32 e 64 bits), Windows 10 (32 e 64 bits) e Mac OS X (v10.10 ou superior).

3.14. REQUISITOS MÍNIMOS SOLUÇÃO DE NGFW – FIREWALL DE PRÓXIMA GERAÇÃO

3.14.1. A plataforma de segurança deve possuir a capacidade e as características abaixo, por equipamento:

3.14.1.1. Throughput de, no mínimo, 35 Gbps com a funcionalidade de firewall e controle de aplicação habilitada para tráfego IPv4 e IPv6, independentemente do tamanho do pacote;

3.14.1.2. Throughput de controle de aplicação de 27 Gbps com tráfego HTTP, 64 Kbytes;

3.14.1.3. Suporte a, no mínimo, 8M conexões simultâneas;

3.14.1.4. Suporte a, no mínimo, 200 novas conexões por segundo;

3.14.1.5. Throughput de, no mínimo, 14 Gbps de VPN IPSec;

3.14.1.6. Estar licenciado para, ou suportar sem o uso de licença, 20K túneis de VPN IPSEC Site-to-Site simultâneos;

3.14.1.7. Estar licenciado para, ou suportar sem o uso de licença, 64K túneis de clientes VPN IPSEC simultâneos;

3.14.1.8. Throughput de, no mínimo, 8 Gbps de VPN SSL;

3.14.1.9. Suporte a, no mínimo, 30K clientes de VPN SSL simultâneos;

3.14.1.10. Suportar no mínimo 20 Gbps de throughput de IPS;

3.14.1.11. Suportar no mínimo 15 Gbps de throughput de Inspeção SSL;

3.14.1.12. Throughput de, no mínimo, 11 Gbps com as seguintes funcionalidade habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS, Antivírus e Antispyware. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito;

3.14.1.13. Possuir ao menos 2 interfaces 1Gbps para gerenciamento;

3.14.1.14. Possuir ao menos 16 interfaces 10Gbps;

3.14.1.15. Disco de, no mínimo, 480 GBytes para armazenamento de informações locais

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

3.14.1.17. Suporte a, no mínimo, 125 sistemas virtuais lógicos (Contextos) por appliance;

3.14.1.18. Deverá acompanhar pelo menos 10 adaptadores Gbics 10Gbps do tipo SR por equipamento;

3.14.1.19. Fonte 120/240 AC ou DC, conforme disponível no local de instalação, redundante e hot-swappble;

3.15. CONSOLE DE GERÊNCIA E MONITORAÇÃO

3.15.1. Deve suportar receber logs de, no mínimo, 2K dispositivos;

3.15.2. Possuir capacidade de receber, no mínimo, 500 GBytes de logs diários;

3.15.3. Suportar, no mínimo, 7500 logs/segundo de forma contínua;

3.15.4. Permitir acesso simultâneo de administradores permitindo a criação de ao menos 2 (dois) perfis para administração e monitoração;

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

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

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

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

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

3.15.10. Autenticação integrada a servidor Radius;

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

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

3.15.13. Autenticação integrada ao Microsoft Active Directory;

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

3.15.15. Deve possuir um assistente para adicionar dispositivos via interface gráfica usando o IP, login e senha dos mesmos;

3.15.16. Deve ser possível visualizar a quantidade de logs enviado de cada dispositivo monitorado;

3.15.17. Possuir mecanismo para que logs antigos sejam removidos automaticamente;

3.15.18. Permitir a importação e exportação de relatórios;

3.15.19. Deve possuir a capacidade de criar relatórios nos formatos HTML;

3.15.20. Deve possuir a capacidade de criar relatórios nos formatos PDF;

3.15.21. Deve possuir a capacidade de criar relatórios nos formatos XML

3.15.22. Deve possuir a capacidade de criar relatórios nos formatos CSV;

3.15.23. Deve ser possível exportar os logs em CSV;

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

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

3.15.26. A solução deve possuir relatórios pré-definidos;

3.15.27. Possuir envio automático de logs para um servidor FTP externo a solução;

3.15.28. Possibilitar a duplicação de relatórios existentes e edita-los logo após;

3.15.29. Possuir a capacidade de personalização de capas para os relatórios;

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

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

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

3.15.33. Deve possuir mecanismo "Drill-Down" para navegação nos relatórios em tempo real;

3.15.34. Dever ser possível fazer download dos arquivos de logs recebidos;

3.15.35. Deve possuir agendamento para gerar e enviar automaticamente relatórios;

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

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

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

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

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

3.15.41. Deve ser possível definir filtros nos relatórios;

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

3.15.43. Permitir que relatórios criado sejam no idioma Português;

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

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

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

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

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

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

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

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

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

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

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

3.15.55. Deve permitir ver em tempo real os logs recebidos;

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

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

3.15.58. Deve possuir relatório de PCI DSS Compliance;

3.15.59. Deve possuir relatório de utilização de aplicações SAAS;

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

3.15.61. Deve possuir relatório de VPN;

3.15.62. Deve possuir relatório de Sistemas de prevenção de intrusão (IPS);

3.15.63. Deve possuir relatório de reputação do cliente;

3.15.64. Deve possuir relatório de análise de segurança do usuário;

3.15.65. Deve possuir relatório de avaliação da ameaça cibernética;

3.15.66. Deve possuir relatório de WiFi PCI Compliance;

3.15.67. Deve possuir relatório a informação de AP´s e SSID´s autorizados, também clientes WiFi;

3.15.68. Deve possuir relatório de equipamentos terminais de solução de segurança gerenciada;

3.15.69. Deve possuir relatório de análise de segurança e uso de web, se há uma plataforma de cache;

3.15.70. Deve possuir relatório de análise aplicações web, se há uma plataforma de segurança web.

3.16. MODELO DE PLANILHA DE ATENDIMENTO A REQUISITOS

3.16.1. O atendimento a todos os itens deve ser comprovado através de documentação oficial do fabricante da solução, que deverá ser anexada à proposta comercial ajustada. A instituição poderá realizar diligência junto ao fabricante para comprovar a autenticidade da documentação. A localização da comprovação na(s) página(s) deverá ser clara e precisa. O não atendimento destes requisitos implicará na desclassificação da proposta.

Item	Documento	Página	Localização

3.17. DOS SERVIÇOS DE MANUTENÇÃO E ASSISTÊNCIA TÉCNICA

3.17.1. O período de prestação de serviços de manutenção e assistência técnica deverá ser de 36 (trinta e seis) meses, contado a partir da data de assinatura do contrato;

3.17.2. Forma de Atendimento da Assistência Técnica:

3.17.2.1. A Contratada deverá disponibilizar “Central de Atendimento” para abertura de chamado de assistência técnica, em dias úteis (segunda-feira à sexta-feira), em horário comercial (08h às 18h), indicando telefone 0800, ou número local em Fortaleza-CE. Os chamados poderão ser abertos pela equipe técnica da contratante.

3.17.2.2. O atendimento será do tipo on-site (no local) mediante manutenção corretiva na localidade de entrega dos itens deste Termo de Referência, incluindo serviços e peças, com janela de atendimento de 24x7, 24 (Vinte e Quatro) horas (00h às 23h59min) e 07 (Sete) dias por semana (Segunda à Segunda), com Tempo de Solução de

até 48 (quarenta e oito) horas. O atendimento deverá ser realizado por profissionais especializados e deverá cobrir todo e qualquer defeito apresentado, incluindo o fornecimento e a substituição de peças e/ou componentes, ajustes, reparos e correções necessárias;

3.17.2.3. A substituição de peças e/ou componentes mecânicos ou eletrônicos de marcas e/ou modelos diferentes dos originais cotados pela contratada, desde que o fabricante assegure que não haverá perda da garantia, somente poderá ser efetuada mediante análise e autorização da contratante.

3.17.2.4. Todas as peças e componentes mecânicos ou eletrônicos substitutos deverão apresentar padrões de qualidade e desempenho iguais ou superiores aos utilizados na fabricação do(s) equipamento(s), sempre “novos e de primeiro uso”, não podendo ser recondicionados.

CLÁUSULA QUARTA – DA FORMA DE FORNECIMENTO

4.1. A entrega do objeto dar-se-á de acordo com os termos estabelecidos na Cláusula Décima do presente instrumento, de acordo com a necessidade da Administração, no quantitativo devidamente identificado na Ordem de Serviço e na respectiva Nota de Empenho.

CLÁUSULA QUINTA – DO VALOR E DO REAJUSTAMENTO DO PREÇO

5.1. O valor contratual global importa na quantia de R$ _____(_____), sujeito a reajustes, desde que observado o interregno mínimo de 01 (um) ano, a contar da apresentação da proposta.

5.2. Caso o prazo exceda a 12 (doze) meses, os preços contratuais serão reajustados utilizando a variação do índice econômico do INPC - Índice Nacional de Preços ao Consumidor do IBGE, ou outro índice em vigor, caso esse seja extinto.

CLÁUSULA SEXTA – DO PAGAMENTO

6.1. O pagamento será efetuado até 30 (trinta) dias contados a partir da lavratura do Termo de Recebimento Definitivo da parcela executada, devidamente atestado pelo gestor da contratação, mediante crédito em conta corrente em nome da contratada, no Banco do Brasil.

6.2. Não será efetuado qualquer pagamento à CONTRATADA, em caso de descumprimento do objeto, conforme especificações exigidas na licitação.

6.3. É vedada a realização de pagamento antes da execução do objeto ou se o mesmo não estiver de acordo com as especificações do Anexo A – Termo de Referência do edital do Pregão Eletrônico n°_____.

6.4. Os pagamentos encontram-se ainda condicionados à apresentação dos seguintes comprovantes:

6.4.1. Documentação relativa à regularidade para com as Fazendas Federal, Estadual e Municipal, o Fundo de Garantia por Tempo de Serviço (FGTS) e a Justiça Trabalhista.

6.5. Toda a documentação exigida deverá ser apresentada em original ou por qualquer processo de reprografia, obrigatoriamente autenticada em cartório. Caso esta documentação tenha sido emitida pela Internet, só será aceita após a confirmação de sua autenticidade.

6.6. A atualização financeira dos valores a serem pagos, em virtude de inadimplemento pela contratante, será efetuada através do INPC (Índice Nacional de Preços ao Consumidor), *pro rata*, desde a data final do período do adimplemento até a data do efetivo pagamento, desde que comprove que o contratante é o único responsável pelo atraso.

CLÁUSULA SÉTIMA – DOS RECURSOS ORÇAMENTÁRIOS

7.1. As despesas decorrentes desta contratação serão provenientes da dotação consignada abaixo:

> **Projeto Atividade: 04.126.0106.1062.0001, Elementos de Despesa: 44.90.39 e 44.9052, Fontes de Recurso: 30101 e 33101, do orçamento da Secretaria Municipal do Planejamento, Orçamento e Gestão – SEPOG.**

CLÁUSULA OITAVA – DO PRAZO DE VIGÊNCIA E DE EXECUÇÃO

8.1. O prazo de vigência deste contrato é de 12 (doze) meses, contado a partir da sua última publicação, devendo ser publicado na forma do parágrafo único, do art. 61, da Lei Federal nº 8.666/1993.

8.2. O prazo de execução do objeto deste contrato é de 12 (doze) meses, contado a partir do recebimento da Ordem de Serviço, após a emissão de empenho.

8.3. Os prazos de vigência e de execução deste contrato poderão ser prorrogados nos termos do que dispõe o art. 57, inciso IV, da Lei Federal n° 8.666/1993.

CLÁUSULA NONA – DA GARANTIA CONTRATUAL

9.1. A garantia prestada, de acordo com o estipulado no edital, será restituída e/ou liberada após o cumprimento integral de todas as obrigações contratuais e, quando em dinheiro, será atualizada monetariamente, conforme dispõe o § 4º, do art. 56, da Lei Federal nº 8.666/1993. Na ocorrência de acréscimo contratual de valor, deverá ser prestada garantia proporcional ao valor acrescido, nas mesmas condições estabelecidas no **item 27** do edital.

CLAÚSULA DÉCIMA – DA ENTREGA E DO RECEBIMENTO

10. DA ENTREGA E DO RECEBIMENTO

10.1. Quanto à entrega:

10.1.1. O objeto contratual deverá ser entregue em conformidade com as especificações estabelecidas neste instrumento, nos locais indicados pela Coordenadoria de Gestão Corporativa de Tecnologia da Informação da Secretaria Municipal do Planejamento, Orçamento e Gestão.

10.1.2. O prazo de entrega do objeto a ser adquirido pelo órgão contratante será de **até 30 (trinta) dias,** contados do recebimento pela empresa da ordem de fornecimento/serviço.

10.1.3. Os atrasos ocasionados por motivo de força maior ou caso fortuito, desde que justificados até 2 (dois) dias úteis antes do término do prazo de entrega, e aceitos pela contratante, não serão considerados como inadimplemento contratual.

10.1.4. A responsabilidade administrativa pelo recebimento do objeto tal qual estipulado no edital será exclusiva da servidor/Comissão de Fiscalização designada pelo órgão participante, encarregada de acompanhar a execução do processo de entrega e recebimento dos objetos do contrato, conforme art. 67 da Lei 8.666/93.

10.1.5. Os equipamentos deverão ser entregues rigorosamente de acordo com as especificações estabelecidas no Anexo A – Termo de Referência deste edital, bem como na proposta vencedora, sendo que a não observância destas condições, implicará na não aceitação do mesmo, sem que caiba qualquer tipo de reclamação ou indenização por parte da inadimplente.

10.1.6. A CONTRATANTE designará um servidor/comissão, cujo propósito será o acompanhamento da entrega e a conferência desta com as especificações contidas na proposta de preços e no Termo de Referência. Caso o objeto esteja em desacordo com as especificações contidas naqueles instrumentos, será rejeitado o recebimento do mesmo.

10.1.7. Devem ser entregues juntamente com os equipamentos, a documentação técnica (impressa ou em CD), incluindo manuais de configuração, CDs, DVDs.

10.2. Quanto ao recebimento:

10.2.1. **PROVISORIAMENTE**, até 10 (dez) dias da entrega do produto, mediante Termo de Recebimento Provisório, para efeito de posterior verificação da conformidade do objeto com as especificações, devendo ser feito pelo(s) fiscal(is) do contrato.

10.2.2. **DEFINITIVAMENTE**, até 30 (trinta) dias da expedição do termo de recebimento provisório, após a verificação da qualidade e da quantidade do objeto, certificando-se de que todas as condições estabelecidas foram atendidas e, consequente aceitação das notas fiscais pelo(s) fiscal(is) da contratação, será expedido termo de recebimento definitivo, devendo haver rejeição do objeto no caso de desconformidade. O Termo de recebimento definitivo será lavrado pelo(s) fiscal(is) do contrato.

10.2.2.1 A nota fiscal/fatura que apresente incorreções será devolvida à contratada para as devidas correções, no prazo estabelecido pela Administração. Nesse caso, o termo de recebimento definitivo somente poderá ser emitido após a referida correção.

10.2.3. O recebimento dos produtos, em caráter provisório ou definitivo, será realizado de segunda a sexta-feira, no horário de 8h às 12h. e de 13h ás 17h

10.2.4. A Administração rejeitará, no todo ou em parte, a entrega dos bens em desacordo com as especificações técnicas exigidas.

10.2.5. Em caso de troca do objeto a mesma deverá ser efetuada no endereço do órgão contratante.

10.2.6. O Contratado deverá providenciar a troca do objeto no prazo máximo de 2 (dois) dias do registro da ocorrência.

10.2.7. A rejeição do objeto por estar em desacordo com as especificações, que vier a ocorrer, não justificará possível atraso no prazo de entrega fixado, sujeitando o licitante vencedor às sanções previstas

CLÁUSULA DÉCIMA PRIMEIRA – DAS OBRIGAÇÕES DA CONTRATADA

11.1. Executar o objeto em conformidade com as condições deste instrumento.

11.2. Manter durante toda a execução contratual, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação.

11.3. Aceitar, nas mesmas condições contratuais, os percentuais de acréscimos ou supressões limitados ao estabelecido no §1º, do art. 65, da Lei Federal nº 8.666/1993, tomando-se por base o valor contratual.

11.4. Responsabilizar-se pelos danos causados diretamente à contratante ou a terceiros, decorrentes da sua culpa ou dolo, quando da execução do objeto, não podendo ser arguido para efeito de exclusão ou redução de sua responsabilidade o fato de a contratante proceder à fiscalização ou acompanhar a execução contratual.

11.5. Responder por todas as despesas diretas e indiretas que incidam ou venham a incidir sobre a execução contratual, inclusive as obrigações relativas a salários, previdência social, impostos, encargos sociais e outras providências, respondendo obrigatoriamente pelo fiel cumprimento das leis trabalhistas e específicas de acidentes do trabalho e legislação correlata, aplicáveis ao pessoal empregado na execução contratual.

11.6. Responder por todos os prejuízos, perdas e danos que venham a ocorrer referentes ao transporte e entrega dos produtos.

11.7. Prestar imediatamente as informações e os esclarecimentos que venham a ser solicitados pela contratante, salvo quando implicarem em indagações de caráter técnico, hipótese em que serão respondidas no prazo de 24 (vinte e quatro) horas.

11.8. Substituir ou reparar o objeto contratual que comprovadamente apresente condições de defeito ou em desconformidade com as especificações deste termo, no prazo máximo de 2 (dois) dias do registro da ocorrência.

11.9. Caso o material, objeto da troca do item anterior, também apresente defeito, o dever de substituí-lo é no prazo máximo de **2 (dois) dias.**

11.10. Cumprir, quando for o caso, as condições de garantia do objeto, responsabilizando-se pelo período oferecido em sua proposta de preços, observando o prazo mínimo exigido pela Administração.

11.11. Os produtos deverão vir lacrados de forma a proteger da ação da luz, poeira umidade, sendo que, nos casos das embalagens apresentarem violação de qualquer espécie, deverão ser substituídas pelo fornecedor, ainda que na fase de análise/recebimento.

11.12. Providenciar a substituição de qualquer empregado que esteja a serviço da contratante, cuja conduta seja considerada indesejável pela fiscalização da contratante.

11.13. Entregar os materiais em conformidade com o presente Termo de Referência e com a proposta em **até 30 (trinta) dias,** contados do recebimento pela empresa da ordem de fornecimento/serviço.

11.14. Discriminar na nota fiscal as especificações do material de modo idêntico àquele apresentado na proposta.

11.15. Não transferir a outrem, por qualquer forma, nem mesmo parcialmente, em subcontratar, qualquer das prestações a que está obrigada por força deste Termo de Referência e seus anexos.

11.16. Assegurar a garantia estipulada, não inferior a 12 (doze) meses, contra defeitos de fabricação, independente de ser ou não o fabricante, devendo providenciar a correção ou a substituição de todos os materiais adquiridos que apresentarem defeitos ou divergência com as especificações fornecidas.

11.17. Arcar com todas as despesas decorrentes do fornecimento dos equipamentos nos locais indicados, e, ainda, com todos os encargos diretos e indiretos que incidir sobre a comercialização dos materiais e seus elementos suplementares e eventuais substituições/ reposições.

11.18. Ressarcir qualquer dano ou prejuízo causado à contratante e/ou a terceiros, provocados por ação ou omissão, ineficiência ou irregularidade cometidas por seus empregados, convenentes, envolvidos na execução do contrato, bem como, assumir inteira responsabilidade civil, administrativa e penal por qualquer prejuízo, material ou pessoal, causados à contratante ou a terceiros.

11.19. Aceitar, sem restrições, a fiscalização da Contratante, no que diz respeito ao fiel cumprimento das condições de fornecimento dos equipamentos.

11.20. Manter-se, durante todo o período de vigência da Ata / Contrato a ser firmado, um preposto aceito pela Contratante, para representação do licitante vencedor sempre que for necessário e comunicando, por escrito, à Contratante qualquer mudança de endereço ou telefone contato.

11.21. Acatar as orientações da Contratante, sujeitando-se a mais ampla e irrestrita fiscalização, prestando os esclarecimentos solicitados e atendendo às reclamações formuladas.

CLÁUSULA DÉCIMA SEGUNDA– DAS OBRIGAÇÕES DA CONTRATANTE

12.1. Solicitar a execução do objeto à CONTRATADA através da emissão de Ordem de Fornecimento/Serviço, após emissão de empenho.

12.2. Proporcionar à CONTRATADA todas as condições necessárias ao pleno cumprimento das obrigações decorrentes do objeto contratual, consoante estabelece a Lei Federal no 8.666/1993 e suas alterações posteriores.

12.3. Fiscalizar a execução do objeto contratual, através de sua unidade competente, podendo, em decorrência, solicitar providências da CONTRATADA, que atenderá ou justificará de imediato.

12.4. Notificar a CONTRATADA de qualquer irregularidade decorrente da execução do objeto contratual.

12.5. Efetuar os pagamentos devidos à CONTRATADA nas condições estabelecidas neste Termo.

12.6. Aplicar as penalidades previstas em lei e neste instrumento.

12.7. Receber os materiais entregues pela contratada que estejam em conformidade com a proposta aceita.

12.8. Recusar, com a devida justificativa, qualquer material entregue fora das especificações constantes neste Termo de Referência.

12.9. Fornecer, mediante solicitação escrita da contratada, informações adicionais, dirimir dúvidas e orientá-la nos casos omissos.

CLÁUSULA DÉCIMA TERCEIRA – DA FISCALIZAÇÃO

13.1. A execução contratual será acompanhada e fiscalizada pelo(a)s Sr(a)s. _____, _____, especialmente designado para este fim pela CONTRATANTE, de acordo com o estabelecido no art. 67, da Lei Federal nº 8.666/1993, doravante denominado simplesmente de GESTOR.

CLÁUSULA DÉCIMA QUARTA – DAS SANÇÕES ADMINISTRATIVAS

14.1. O contratado que praticar ato ilícito estará sujeito, garantido o direito prévio de citação e da ampla defesa, sem prejuízo das sanções legais nas esferas civis e criminais, às seguintes penalidades, de acordo com o Decreto Municipal nº 13.735/2016:

I. Advertência, que consista em comunicação formal ao infrator, decorrente da inexecução de deveres que ocasionem riscos e/ou prejuízos de menor potencial ofensivo para a Administração;

II. Multa cumulativa com as demais sanções, conforme estabelecido nos artigos 50 e 51 do Decreto Municipal nº 13.375/2016

III. Impedimento de licitar e contratar com a Administração Direta e Indireta do Município de Fortaleza e descredenciamento no Cadastro de Fornecedores da Central de Licitações da Prefeitura de Fortaleza - CLFOR, pelo prazo de até 05 (cinco) anos.

14.1.1. Entende-se por ato ilícito qualquer conduta comissiva ou omissiva que infrinja dispositivos legais ou regras constantes de regulamentos ou de qualquer outro ato normativo, inclusive aquelas constantes dos atos convocatórios de licitação, da ata de registro de preços, do contrato ou instrumento que o substitua.

14.1.2. A aplicação das multas de natureza moratória não impede a aplicação superveniente de outras multas previstas neste item, cumulando-se os respectivos valores.

14.1.3. O atraso, para efeito de cálculo da multa, será contado em dias corridos, a partir do primeiro dia útil subsequente ao do encerramento do prazo estabelecido para o cumprimento da obrigação

14.1.4. No caso de prestações continuadas, a multa de 5% (cinco por cento) de que trata a alínea "d" deste item será calculada sobre o valor da parcela que eventualmente for descumprida.

14.1.5. A critério da autoridade competente, o valor da multa poderá ser descontado do pagamento a ser efetuado ao contratado, inclusive antes da execução da garantia contratual, quando esta não for prestada sob a forma de caução em dinheiro.

14.1.6. Caso o valor a ser pago ao contratado seja insuficiente para satisfação da multa, a diferença será descontada da garantia contratual.

14.1.7. Caso a faculdade prevista no subitem 14.1.5 não tenha sido exercida e verificada a insuficiência da garantia para satisfação integral da multa, o saldo remanescente será descontado de pagamentos devidos ao contratado.

14.1.8. Caso o valor da garantia seja utilizado, no todo ou em parte, para o pagamento da multa, esta deve ser complementada pelo contratado no prazo de até 10 (dez) dias uteis, a contar da solicitação do contratante.

14.1.9. Após esgotados os meios de execução direta da sanção de multa, o licitante será notificado para recolher a importância devida no prazo de 15 (quinze) dias, contados do recebimento da comunicação oficial. Decorrido o prazo, a CLFOR encaminhará a multa para que seja inscrita na Dívida Ativa do Município.

14.2. Na aplicação das sanções devem ser consideradas as seguintes circunstancias:

I. a natureza e a gravidade da infração cometida;

II. os danos que o cometimento da infração ocasionar aos serviços e aos usuários;

III. a vantagem auferida em virtude da infração;

IV. as circunstancias gerais agravantes e atenuantes;

V. os antecedentes da licitante ou contratada.

CLÁUSULA DÉCIMA QUINTA – DA RESCISÃO CONTRATUAL

15.1. A inexecução total ou parcial deste contrato e a ocorrência de quaisquer dos motivos constantes no art. 78, da Lei Federal nº 8.666/1993 será causa para sua rescisão, na forma do art. 79, com as consequências previstas no art. 80, do mesmo diploma legal.

15.2. Este contrato poderá ser rescindido a qualquer tempo pela CONTRATANTE, mediante aviso prévio de no mínimo 30 (trinta) dias, nos casos das rescisões decorrentes do previsto no inciso XII, do art. 78, da Lei Federal nº 8.666/1993, sem que caiba à CONTRATADA direito à indenização de qualquer espécie.

CLÁUSULA DÉCIMA SEXTA – DO FORO

16.1. Fica eleito o foro do Município de Fortaleza, do Estado do Ceará, para dirimir quaisquer questões decorrentes da execução deste contrato, que não puderem ser resolvidas na esfera administrativa.

E, por estarem de acordo, foi mandado lavrar o presente contrato, que está visado pela Assessoria Jurídica da CONTRATANTE, e do qual se extraíram 2 (duas) vias de igual teor e forma, para um só efeito, as quais, depois de lidas e achadas conforme, vão assinadas pelos representantes das partes e pelas testemunhas abaixo.

Local e data

(nome do representante) (nome do representante)

CONTRATANTE CONTRATADO(A)

Testemunhas:

(nome da testemunha 1) (nome da testemunha 2)

RG: RG:
CPF: CPF:
Visto:

ANEXO F – MODELO DE DECLARAÇÃO RELATIVA AO TRABALHO DE EMPREGADO MENOR

EMPREGADOR PESSOA FÍSICA/PESSOA JURÍDICA

(colocar em papel timbrado quando se tratar de pessoa jurídica)

(Identificação do licitante), inscrito no CPF/CNPJ nº _____, DECLARA, para fins do disposto no inciso V, do art. 27, da Lei Federal nº 8.666, de 21 de junho de 1993, acrescido pela Lei Federal nº 9.854, de 27 de outubro de 1999, que não emprega em trabalho noturno, perigoso ou insalubre, menores de dezoito anos e em qualquer trabalho, menores de dezesseis anos, salvo na condição de aprendiz, a partir de quatorze anos.

Local e data

Assinatura do representante legal

(Nome e cargo)

ANEXO G – MODELO DE ORDEM DE FORNECIMENTO/ SERVIÇO

ORDEM DE SERVIÇO Nº /20__

Nº CONTRATO	**CONTRATADA**	**CNPJ**

OBJETO DO CONTRATO:

ESCOPO DA ORDEM DE SERVIÇO: Descrição do objeto.... , conforme descrito abaixo:

Lote	Produto	Qtd	Vr Unitário R$	Vr Total R$
1				
	TOTAL			**R$**

LOCAL DE ENTREGA:

VALOR DA ORDEM DE SERVIÇO:

VALOR GLOBAL DO CONTRATO: R$

PRAZO DE ENTREGA: De acordo com os prazos estabelecidos no Termo de Referência.

Pela presente ORDEM DE SERVIÇO fica a empresa, autorizada a prestar os serviços objeto do contrato n° /20___, processo nº /2017 discriminado nesta OS.

rtaleza, de de 20___

Matrícula nº
Coordenador Administrativo-Financeiro
ÓRGÃO / ENTIDADE

EMPRESA
CONTRATADO

ANEXO H – DA ANÁLISE DAS AMOSTRAS

1. DOS PRAZOS

1.1. As amostras deverão ser solicitadas pelo pregoeiro ao licitante arrematante do certame.

1.2. Após a solicitação do pregoeiro, o arrematante deverá no prazo de 03 (três) dias úteis, contados a partir da solicitação do pregoeiro, entrar em contato com a Coordenadoria de Gestão Corporativa da Tecnologia da Informação - COGECT da Secretaria Municipal do Planejamento, Orçamento e Gestão, por meio do telefone (85) 3452-3430, para agendar o dia da entrega da amostra e execução das análises.

1.3 A entrega das amostras deverá ocorrer em até 07 (sete) dias úteis do contato mencionado no subitem 1.2, na sede da COGECT/SEPOG localizada no endereço: Rua Tibúrcio Cavalcante, 1233 – Aldeota, Fortaleza/CE, nos horários de 8h às 12h e de 13h às 17h.

1.4 A finalização da análise das amostras ocorrerá em até 05 (cinco) dias úteis, contados a partir do dia subsequente ao dia da entrega da amostra.

1.5 O não cumprimento dos prazos e determinações do subitem 1.2 e 1.3,resultará na desclassificação da licitante.

1.6 A COGECT/SEPOG encaminhará ao pregoeiro do certame o relatório com a avaliação das amostras, em até 02 (dois) dias úteis após o termino do prazo estabelecido no subitem 1.4.

2. DA ANÁLISE

2.1 As amostras serão analisadas por técnicos da Coordenadoria de Gestão Corporativa da Tecnologia da Informação e Comunicação (COGECT)/SEPOG, que verificarão a conformidade das amostras com as especificações técnicas constantes neste edital e com proposta da empresa, devendo emitir laudo devidamente datado e assinado por quem o emitiu, e ratificado pelo titular do órgão.

2.2 A COGECT/SEPOG determinará as especificações que serão verificadas e que estão previstas no Anexo A - Termo de Referência deste Edital, não necessariamente englobando todas as listadas, em função da impossibilidade de teste integral no período e ambiente de execução restritos da fase de amostra.

2.3 As informações tratadas no subitem anterior, serão informadas ao licitante no contato a ser realizado e descrito no subitem 1.2, por meio de e-mail.

2.4. A licitante será aprovada na avaliação caso atenda na íntegra as especificações analisadas. Caso a licitante falhe em atender em pelo menos uma das especificações examinadas, será reprovada na amostra.

2.5 Uma especificação somente será considerada atendida se estiver de acordo com o que está estabelecido no Anexo A – Termo de Referência deste Edital.

3. DAS DISPOSIÇÕES GERAIS

3.1 A não obediência dos dispositivos que versam sobre amostra nesse Edital, será motivo de desclassificação do(s) licitante(s) por não apresentar/disponibilizar amostras dos lotes/itens conforme determinado.

3.2. Será rejeitada a amostra que:

a) apresentar problemas de funcionamento durante a análise técnica;
b) apresentar divergência em relação às especificações técnicas da proposta;
c) não estiver em conformidade com as especificações do Anexo A – Termo de Referência deste Edital.

ANEXO I – GLOSSÁRIO

AD – *Active Directory* é uma implementação de serviço de diretório no protocolo LDAP que armazena informações sobre objetos em rede de computadores e disponibiliza essas informações a usuários e administradores desta rede. É um software da Microsoft utilizado em ambientes Windows, presentes no *active directory*

AGREGAÇÃO DE LINKS – *Ethernet Bonding*, regulado pela norma IEEE 802.3ad com o título link *aggregation* é uma técnica em redes de computadores usada para o acoplamento de dois ou mais canais ethernet em paralelo para produzir um único canal de maior velocidade e/ou aumentar a disponibilidade e redundância desse canal

ANTI SPOOFING – proteção contra IP *Spoofing*

ANTI-SPYWARE - são programas cujo objetivo é tentar eliminar do sistema, através de uma varredura, *spywares*, *adwares*, *keyloggers*, *trojans* e outros *malwares*

ANTIVÍRUS - Programa de computador concebidos para prevenir, detectar e eliminar vírus de computador

API – É um conjunto de rotinas e padrões de programação para acesso a um aplicativo de software ou plataforma baseado na Web. A sigla API refere-se ao termo em inglês "*Application Programming Interface*" que significa em tradução para o português "Interface de Programação de Aplicativos"

APPLIENCE – É um dispositivo de hardware separado e discreto com software integrado (*firmware*), especificamente projetado para fornecer um recurso de computação específico para requisições de clientes solicitando recursos de outros servidores

BGP – é um protocolo de roteamento Inter domínios, criado para uso nos roteadores principais da Internet

BOTNETS - É uma rede de computadores infectados por *malware* que estão sob o controle de uma única parte atacante, conhecida como "pastor de *bots*"

BUFFER OVERFLOW - é uma anomalia onde um programa, ao escrever dados em um buffer, ultrapassa os limites do buffer e sobrescreve a memória adjacente

CACHE - é um dispositivo de acesso rápido, interno a um sistema, que serve de intermediário entre um operador de um processo e o dispositivo de armazenamento ao qual esse operador acede.

CAMADA 2 – A camada de ligação de dados também é conhecida como de enlace ou link de dados. Esta camada detecta e, opcionalmente, corrige erros que possam acontecer no nível físico

CAMADA 3 – A camada de rede fornece os meios funcionais e de procedimento de transferência de comprimento variável de dados de sequências de uma fonte de acolhimento de uma rede para um host de destino numa rede diferente (em contraste com a camada de ligação de dados que liga os

hosts dentro da mesma rede), enquanto se mantém a qualidade de serviço requerido pela camada de transporte

CAMADA 7 – A camada de aplicação corresponde às aplicações (programas) no topo da camada OSI que serão utilizadas para promover uma interação entre a máquina-usuário (máquina destinatária e o usuário da aplicação)

CAPTIVE PORTAL - é um programa de computador responsável por controlar e gerenciar o acesso à Internet em redes públicas, de forma "automatizada"

CLIENT-TO-SITE – Túnel VPN estabelecido entre um host e um *gateway*

CLUSTER – Consiste em computadores vagamente ou fortemente ligados que trabalham em conjunto para que, em muitos aspectos, eles possam ser vistos como um único sistema

CPU – Unidade Central de Processamento ou CPU (*Central Processing Unit*), também conhecido como processador, é a parte de um sistema computacional, que realiza as instruções de um programa de computador, para executar a aritmética básica, lógica, e a entrada e saída de dados

DDoS – Ataque de Negação de Serviço Distribuído

DELAY - É o termo técnico usado para designar o retardo de sinais em circuitos eletrônicos

DHCP – O DHCP, *Dynamic Host Configuration Protocol* (Protocolo de configuração dinâmica de host), é um protocolo de serviço TCP/IP que oferece configuração dinâmica de terminais, com concessão de endereços IP de host, Máscara de sub-rede, Default Gateway (Gateway Padrão), Número IP de um ou mais servidores DNS, Número IP de um ou mais servidores WINS e Sufixos de pesquisa do DNS

DIFFSERV – Ou serviços diferenciados é um método utilizado na tentativa de conseguir qualidade de serviço em grandes redes, como a Internet

DNS - É um sistema de gerenciamento de nomes hierárquico e distribuído para computadores, serviços ou qualquer recurso conectado à Internet ou numa rede privada

DoS – Ataque de Negação de Serviço

DOWNLOAD E UPLOAD – São termos utilizados para referenciar a transmissão de dados de um dispositivo para outro através de um canal de comunicação previamente estabelecido

DROP – Descarte da conexão

ECMP – *Equal-cost multi-path routing*, é um algoritmo para roteamento de dados em uma rede

ETHERNET – É uma arquitetura de interconexão para redes locais - Rede de Área Local (LAN) - baseada no envio de pacotes

EXPLOITS - É um pedaço de software, um pedaço de dados ou uma sequência de comandos que tomam vantagem de um defeito, falha ou vulnerabilidade a fim de causar um comportamento

acidental ou imprevisto a ocorrer no software ou hardware de um computador ou em algum eletrônico (normalmente computadorizado)

FIREWALL – É um dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede

HA – Alta disponibilidade

HARDWARE – é usado para fazer referência a detalhes específicos de uma dada máquina, incluindo-se seu projeto lógico pormenorizado bem como a tecnologia de embalagem da máquina

HASH – É um algoritmo que mapeia dados de comprimento variável para dados de comprimento fixo. Os valores retornados por uma função *hash* são chamados valores *hash*, códigos *hash*, somas *hash* (*hash sums*), *checksums* ou simplesmente *hashes*

ICMP – Sigla para o inglês *Internet Control Message Protocol*, é um protocolo integrante do Protocolo IP, definido pelo RFC 792, é utilizado para fornecer relatórios de erros à fonte original

ICMP FLOOD - É um ataque de negação de serviço simples no qual o atacante sobrecarrega o sistema vítima com pacotes ICMP Echo Request (pacotes ping)

INBOUND – Tráfego de entrada

IP - *Internet Protocol* e é um número que seu computador (ou roteador) recebe quando se conecta à Internet. É através desse número que seu computador é identificado e pode enviar e receber dados

IP SPOOFING - É um ataque que consiste em mascarar (*spoof*) pacotes IP utilizando endereços de remetentes falsificados

IPS - *Intrusion Prevention System* ou, sistema de prevenção a intrusões

IPSec - É uma extensão do protocolo IP que visa a ser o método padrão para o fornecimento de privacidade do usuário (aumentando a confiabilidade das informações fornecidas pelo usuário para uma localidade da internet, como bancos), integridade dos dados (garantindo que o mesmo conteúdo que chegou ao seu destino seja o mesmo da origem) e autenticidade das informações ou prevenção de *identity spoofing* (garantia de que uma pessoa é quem diz ser), quando se transferem informações através de redes IP pela internet

IPv4 – É a versão quatro do protocolo de internet

IPv6 – É a versão seis do protocolo de internet

JUMBO FRAMES – Pacotes jumbo ou quadros jumbo são quadros ethernet com mais de 1500 bytes de carga útil (*payload*), o limite definido pelo padrão IEEE 802.3

LACP – Fornece um método para controlar o agrupamento de várias portas físicas em conjunto para formar um único canal lógico. LACP permite que um dispositivo de rede negocie um agrupamento automático de links enviando pacotes LACP para o dispositivo (dispositivo diretamente conectado que também implementa LACP)

LDAP – *Lightweight Directory Access Protocol*, ou LDAP, é um protocolo de aplicação aberto, livre de fornecedor e padrão de indústria para acessar e manter serviços de informação de diretório distribuído sobre uma rede de Protocolo da Internet (IP)

LOG – Registro de eventos em um sistema de computadores

MULTICAST – É a entrega de informação para múltiplos destinatários simultaneamente usando a estratégia mais eficiente onde as mensagens só passam por um link uma única vez e somente são duplicadas quando o link para os destinatários se divide em duas direções

NAT – *Network Address Translation*, também conhecido como *masquerading* é uma técnica que consiste em reescrever, utilizando-se de uma tabela *hash*, os endereços IP de origem de um pacote que passam por um *router* ou *firewall* de maneira que um computador de uma rede interna tenha acesso ao exterior ou Rede Mundial de Computadores

NGFW - Next Generation Firewall ou, simplesmente, Firewall de Próxima Geração, entende-se o conjunto de funcionalidades de Firewall, IPS, Antivírus, Controle de Aplicação, Filtro de URL, Identificação de usuários e Controle de ameaças avançadas

OSPF – Open Shortest Path First - é um protocolo de roteamento para redes que operam com protocolo IP; desenvolvido pelo grupo de trabalho da IGPs (Interior Gateway Protocol) da IETF (Internet Engineering Task Force) e descrito inicialmente em 1989 pela RFC 1131

OUTBOUND – Tráfego de saída

PAYLOAD – Refere-se à carga de uma transmissão de dados

POLICY BASED ROUTING / POLICY BASED FORWARDING – Roteamento baseado em políticas.

PORTSCANS - São ferramentas com o objetivo de mapear as portas TCP e UDP

PROTOCOLO – É uma convenção que controla e possibilita uma conexão, comunicação, transferência de dados entre dois sistemas computacionais

PROXY - É um servidor (um sistema de computador ou uma aplicação) que age como um intermediário

QoS – Refere-se à garantia de largura de banda

RADIUS - É um protocolo de rede que fornece gerenciamento centralizado de Autenticação, Autorização e Contabilização (*Accounting*, em inglês) para usuários que se conectam a e utilizam um serviço de rede

RIP – É um padrão para troca de informações entre os gateways e hosts de roteamento

ROUND-ROBIN – É um dos algoritmos mais simples de agendamento de processos em um sistema operacional, que atribui frações de tempo para cada processo em partes iguais e de forma circular, manipulando todos os processos sem prioridades. Escalonamento *Round-Robin* é simples e fácil de implementar

SINGLE SIGN-ON - É um mecanismo pelo qual torna-se possível que um usuário obtenha acesso a múltiplos serviços após autenticar-se somente uma vez em qualquer um destes serviços

SITE-TO-SITE – Túnel VPN estabelecido entre dois ou mais *gateways*

SNIFFER – conhecido como analisador de redes, analisador de protocolos ou analisador de *sniffer*.

SNMP – É o protocolo padrão para monitoramento e gerenciamento de redes

SSH – É um protocolo de rede criptográfico para operação de serviços de rede de forma segura sobre uma rede insegura

SSL – *Secure Socket Layer* (SSL) é um padrão global em tecnologia de segurança. Ele cria um canal criptografado entre um servidor web e um navegador (browser) para garantir que todos os dados transmitidos sejam sigilosos e seguros

SSL VPN - É um tipo de VPN que corre ao longo *Transport Layer Security* (TLS) e é acessível com um navegador da Web

SYN FLOOD - Ou ataque SYN é uma forma de ataque de negação de serviço (também conhecido como *Denial of Service* - DoS) em sistemas computadorizados, na qual o atacante envia uma sequência de requisições SYN para um sistema-alvo visando uma sobrecarga direta na camada de transporte e indireta na camada de aplicação do modelo OSI

TAG – Um campo que contém a informação da VLAN (e/ou 802.1p) que pode ser introduzido em um frame da Ethernet

TCP – *Transmission Control Protocol*, que significa "Protocolo de controle de transmissão" é um dos protocolos sob os quais assenta a Internet. Ele é complementado pelo Protocolo da Internet, sendo normalmente chamado de TCP/IP

THROUBLESHOOT - É uma forma de resolver problemas, muitas vezes aplicada na reparação de produtos ou processos falhados

THROUGHPUT - É a quantidade de dados transferidos de um lugar a outro, ou a quantidade de dados processados em um determinado espaço de tempo

TLS – É um protocolo criptográfico cuja função é conferir segurança para a comunicação na Internet para serviços como e-mail (SMTP), navegação por páginas (HTTP) e outros tipos de transferência de dados

TOKENS - É um dispositivo eletrônico gerador de senhas, geralmente sem conexão física com o computador

ToR – É um software livre e de código aberto que proporciona o anonimato pessoal ao navegar na Internet e em atividades online, protegendo contra a censura e principalmente a privacidade pessoal

TRAFFIC SHAPING – É um termo da língua inglesa (modelagem do tráfego), utilizado para definir a prática de priorização do tráfego de dados, através do condicionamento do débito de redes, a fim de otimizar o uso da largura de banda disponível

UDP FLOOD - É um ataque de negação de serviço usando UDP (*User Dtatagram Protocol*)

URL - É uma sigla correspondente às palavras inglesas "*Uniform Resource Locator*". Um URL se refere ao endereço de rede no qual se encontra algum recurso informático

VLAN – Padrão que permite a criação de redes virtuais locais (VLANs) dentro de uma rede *ethernet* (802.1q)

VoIP – É o roteamento de conversação humana usando a Internet ou qualquer outra rede de computadores baseada no Protocolo de Internet, tornando a transmissão de voz mais um dos serviços suportados pela rede de dados

VPN – É uma rede de comunicações privada construída sobre uma rede de comunicações pública

WEB – Sistema hipertextual que opera através da internet

WORMS - É um programa autorreplicante, diferente de um vírus