EDITAL DE PREGÃO ELETRÔNICO Nº 148/2018.

Processo Administrativo nº: 033763/2018.

OBJETO: Contratação de empresa especializada e tecnicamente qualificada para prestação dos serviços de fornecimento e implantação de solução de segurança e conectividade (*hardwares* - equipamentos e *softwares* - sistemas) para as áreas de tecnologia da informação da Prefeitura Municipal de Foz do Iguaçu, incluindo-se o fornecimento de equipamentos e sistemas necessários para a ampliação e/ou a substituição de ativos de rede, *internet*, *firewall*, *switches* e roteadores, bem como *softwares* e demais sistemas necessários, conforme descrição e quantitativos estabelecidos neste Termo de Referência e seus anexos.

Valor máximo estimado por 12 meses: R$ 2.203.362,15 (Dois milhões, duzentos e três mil, trezentos e sessenta e dois reais, e quinze centavos)**.**

DATAS RELATIVAS AO CERTAME

- **Pedidos de esclarecimentos**: até 3 (três) dias úteis antes do recebimento das propostas[1];
- **Impugnações**: até 2 (dois) dias úteis antes do recebimento das propostas;
- **Recebimento das propostas**: até às 14:30 horas do dia 12/09/2018;
- **Abertura e avaliação das propostas**: dia 12/09/2018, a partir das 14:30 horas;
- **Início da sessão pública / lances**: dia 12/09/2018, ás 14h45min.

ENDEREÇOS

PREGOEIRO: Natanael de Almeida.
Fone: (45) 3521-1369 - natanael.na@pmfi.pr.gov.br
Horário de expediente: das 08h00 / 12:00 e das 13:30 ás 17:30 horas.
Praça Getulio Vargas, nº 260 - Foz do Iguaçu - PR.
Acesso identificado no link - www.licitacoes-e.com.br

ANEXOS INTEGRANTES DO EDITAL

Integram este Edital, como se nele estivessem transcritos, os anexos abaixo relacionados, dispostos na seguinte ordem:

a) ***Anexo I*** *- Termo de Referência;*
b) ***Anexo II*** *- Das exigências da proposta comercial e da habilitação;*
c) ***Anexo III*** *- Minuta de Contrato;*
d) ***Modelo I*** *- Declaração de cumprimento do art. 3º da L.C 123/06 e alterações;*

[1] Os pedidos de esclarecimentos, as respostas do Pregoeiro e eventuais adendos serão postados no portal licitações-e, para consulta dos licitantes.

e) ***Modelo II*** *- Declaração Conjunta;*

f) ***Modelo III*** *- Declaração de Elaboração Independente de Proposta;*

g) ***Modelo IV*** *- Proposta Comercial;*

h) ***Modelo V*** *- Capacidade financeira;*

PREÂMBULO

O Município de Foz do Iguaçu - PR, com sede na Praça Getulio Vargas nº 260 - Centro - CEP 85.851-340 torna público para conhecimento de todos os interessados, que no dia e hora indicadas, será realizada licitação na modalidade Pregão Eletrônico, do tipo **menor preço,** que será regido pela Lei Federal n.º 10.520, de 17/07/2002, Decreto Municipal nº 19.302 de 04 de dezembro de 2009, Decreto Municipal nº 18.718 de 26 de fevereiro de 2009, com aplicação subsidiária da Lei Federal nº 8.666/93 e suas alterações, além das demais disposições legais aplicáveis e do disposto no presente Edital.

1. DAS DISPOSIÇÕES E RECOMENDAÇÕES PRELIMINARES

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

1.2. Os trabalhos serão conduzidos por funcionário da Prefeitura do Município de Foz do Iguaçu, denominado Pregoeiro, mediante a inserção e monitoramento de dados gerados ou transferidos para o aplicativo "Licitações" constante da página eletrônica do Banco do Brasil S.A. **www.licitacoes-e.com.br**

1.3. Os interessados que tiverem dúvidas de caráter técnico ou legal quanto à interpretação dos termos deste Edital poderão solicitar esclarecimentos, providências ou impugnar em até 02 (dois) dias úteis antes da data fixada para recebimento das propostas, preferencialmente pelo e-mail natanael.na@pmfi.pr.gov.br, ou através de correspondência dirigida ao endereço constante preâmbulo do Edital. *Os esclarecimentos prestados pelo Pregoeiro serão estendidos aos demais licitantes que manifestaram intenção de participação no processo licitatório*. Caso seja acolhida a impugnação contra o ato convocatório, será designada nova data para a realização do certame, exceto quando resultar alteração no edital e esta, inquestionavelmente, não afetar a formulação das propostas.

1.4. Qualquer cidadão é parte legítima para impugnar este Edital, devendo, neste caso, protocolar pedido até **2** (dois) dias úteis antes da data fixada para a abertura da licitação, devendo, o Pregoeiro julgar e responder à impugnação em até 24 (vinte e quatro) horas.

1.5. O presente edital se submete ao disposto na Lei Complementar 123/2006 e alterações posteriores, que estabelecem normas relativas ao tratamento diferenciado e favorecido às microempresas e empresas de pequeno porte.

1.6. Caberá ao licitante interessado em participar do pregão, na forma eletrônica, acompanhar as operações no sistema eletrônico durante o processo licitatório, responsabilizando-se pelo ônus decorrente da perda de negócios diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão (art. 13, IV do Decreto 5.450/05);

1.7. A utilização dos benefícios concedidos pela LC nº 123/2006 e alterações posteriores, por licitante que não se enquadra na definição legal reservada a essas categorias, configura fraude ao certame, sujeitando a mesma à aplicação de penalidade de impedimento de licitar e contratar com o Município de Foz do Iguaçu - PR, pelo prazo de até 5 (cinco) anos, sem prejuízo das multas previstas neste Edital e das demais cominações legais.

1.8. O prazo de execução dos serviços será de 12 (doze) meses, contados a partir da data da assinatura, podendo ser prorrogado por igual período nas mesmas condições iniciais, conforme disposto no artigo 57, II, da Lei nº. 8.666/93 e alterações posteriores.

2. DAS CONDIÇÕES PARA PARTICIPAÇÃO

2.1. Poderão participar desta Licitação qualquer firma individual ou sociedade, regularmente estabelecida no País, que seja especializada no objeto desta licitação e que satisfaça todas as exigências, especificações e normas contidas neste Edital e seus Anexos.

2.2. Empresas constituídas na forma de consórcio ou isoladamente.

2.3. Não poderá participar da licitação a empresa que estiver sob falência, concordata, recuperação judicial e extrajudicial, dissolução, liquidação ou que esteja suspensa de licitar e/ou contratar com a Administração Pública ou impedida legalmente.

2.4. Estarão impedidos de participar de qualquer fase do processo, os licitantes que se enquadrem em uma ou mais das situações a seguir:

2.3.1 Empresas suspensas de participar de licitação e impedidas de contratar com o Município de Foz do Iguaçu, durante o prazo da sanção aplicada;
2.3.2 Empresa declarada inidônea para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida sua reabilitação;
2.3.3 Empresa proibida de contratar com o Poder Público, em razão do disposto no art.72, § 8º, V, da Lei nº 9.605/98;
2.3.4 Empresa proibida de contratar com o Poder Público, nos termos do art. 12 da Lei nº 8.429/92;
2.3.5 Quaisquer interessados enquadrados nas vedações previstas no art. 9º da Lei nº 8.666/93. Entende-se por "participação indireta" a que alude o art. 9º da Lei nº 8.666/93 a participação no certame de empresa em que uma das pessoas listadas no mencionado dispositivo legal figure como sócia, pouco importando o seu conhecimento técnico acerca do objeto da licitação ou mesmo a atuação no processo licitatório.
2.3.6 Sociedade estrangeira não autorizada a funcionar no País;
2.3.7 Empresa que se encontre em processo de dissolução, recuperação judicial, recuperação extrajudicial, falência, fusão, cisão, ou incorporação.
Consórcio.

2.5. A microempresa ou empresa de pequeno porte, além da apresentação da declaração constante no **modelo I** para fins de habilitação, deverá, quando do cadastramento da proposta inicial de preço a ser digitado no sistema, informar o seu regime de tributação para efeitos de tratamento diferenciado e favorecido nos termos da Lei Complementar 123/2006.

2.6. O encaminhamento de proposta pressupõe o pleno conhecimento e atendimento às exigências de habilitação previstas no Edital. O fornecedor será responsável por todas as transações que forem efetuadas em seu nome no sistema eletrônico, assumindo como firmes e verdadeiras suas propostas e lances;

2.7. A validade da proposta será de no mínimo **60 (sessenta) dias**, contados a partir da data da sessão pública do Pregão.

3. DO OBJETO

3.1. Consta do **Anexo I** deste Edital a especificação completa do objeto.

4. DA CONDUÇÃO DO CERTAME PELO MUNICÍPIO

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

I - Recebimento das propostas de preços e da documentação de habilitação;
II - A abertura das propostas de preços, o seu exame e a classificação dos licitantes;
III - A condução dos procedimentos relativos aos lances e à escolha da proposta ou do lance de menor preço;
IV - A adjudicação da proposta de menor preço;
V - A elaboração de ata;
VI - A condução dos trabalhos da equipe de apoio;
VII - Recebimento, exame e decisão sobre recursos;
VIII - Encaminhamento do processo devidamente instruído, após a adjudicação, à autoridade superior, visando à homologação e a contratação.

5. DOS PROCEDIMENTOS NO PORTAL ELETRÔNICO

5.1. Para acesso ao sistema eletrônico, os interessados em participar do Pregão deverão dispor de chave de identificação e senha pessoal (*intransferíveis*), obtida através do site **www.licitacoes-e.com.br**

5.2. A participação no Pregão Eletrônico se dará por meio da digitação da senha pessoal e intransferível do representante credenciado e subsequente encaminhamento da proposta de preços, exclusivamente por meio do sistema eletrônico, observados data e horário e limite estabelecidos. Obs. a informação dos dados para acesso deve ser feita na página inicial do site **www.licitacoes-e.com.br**.

5.3. O credenciamento do fornecedor e de seu representante legal junto ao sistema eletrônico implica a responsabilidade legal pelos atos praticados e a presunção de capacidade técnica para realização das transações inerentes ao pregão eletrônico.

5.4. É de exclusiva responsabilidade do usuário o sigilo da senha, bem como seu uso em qualquer transação efetuada diretamente ou por seu representante, não cabendo ao provedor do sistema ou ao órgão promotor da licitação responsabilidade por eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros.

5.5. O credenciamento do fornecedor e de seu representante legal junto ao sistema eletrônico

implica a responsabilidade legal pelos atos praticados e a presunção de capacidade técnica para realização das transações inerentes ao pregão eletrônico.

5.6. Caberá ao fornecedor acompanhar as operações no sistema eletrônico durante a sessão pública do pregão, ficando responsável pelo ônus decorrente da perda de negócios diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão.

6. ABERTURA DAS PROPOSTAS E FORMULAÇÃO DOS LANCES

6.1. A partir do horário previsto no Edital e no sistema para cadastramento e encaminhamento da proposta inicial de preço terá início a sessão pública do Pregão Eletrônico, com a divulgação das propostas de preços recebidas, passando o Pregoeiro a avaliar a aceitabilidade das propostas. Previamente à etapa de abertura de propostas, o licitante deverá certificar-se de que sua proposta foi inserida corretamente no sistema, cuja visualização possa ser realizada tanto pelos demais licitantes como pelo Pregoeiro. A não visualização pelo Pregoeiro, independentemente da razão, será considerada como não inserida, acarretando na desclassificação do licitante.

6.2 Após a sessão de lances, não serão aceitas propostas com valores superiores ao máximo fixado no Edital. O descumprimento desse requisito implicará na desclassificação do licitante.

6.3. Aberta a etapa competitiva, os representantes dos fornecedores deverão estar conectados ao sistema para participar da sessão de lances. A cada lance ofertado o participante será imediatamente informado de seu recebimento e respectivo horário de registro e valor.

6.4. O fornecedor poderá encaminhar lance com valor superior ao menor lance registrado, desde que seja inferior ao seu último lance ofertado e diferente de qualquer lance válido para o lote.

6.5. Não serão aceitos dois ou mais lances de mesmo valor, prevalecendo aquele que for recebido e registrado em primeiro lugar.

6.6. Durante o transcurso da sessão pública, os participantes serão informados, em tempo real, do valor do menor lance registrado. O sistema **não identificará** o autor dos lances aos demais participantes.

6.7. No caso de desconexão com o Pregoeiro, no decorrer da etapa competitiva do Pregão Eletrônico, o sistema eletrônico poderá permanecer acessível aos licitantes para a recepção dos lances, retornando o Pregoeiro, quando possível, sua atuação no certame, sem prejuízos dos atos realizados.

6.8. Quando a desconexão persistir por tempo superior a dez minutos, a sessão do Pregão Eletrônico será suspensa e terá reinício somente após comunicação expressa aos participantes, através de mensagem eletrônica (*e-mail*) divulgando data e hora da reabertura da sessão.

6.9. A etapa inicial de lances da sessão pública será encerrada mediante aviso de fechamento iminente dos lances, emitido pelo sistema eletrônico, após o que transcorrerá período de tempo extra. O período de tempo extra, ocorrerá em um intervalo que poderá ser de 0 (zero) a 30 (trinta) minutos, aleatoriamente determinado pelo sistema eletrônico, findo o qual será automaticamente encerrada a recepção de lances, não podendo, em hipótese alguma, as empresas apresentarem novos lances.

6.10. Devido à imprevisão de tempo extra, as empresas participantes deverão estimar o seu valor mínimo de lance a ser ofertado, evitando assim, cálculos de última hora, que poderá resultar em uma disputa frustrada por falta de tempo hábil**.**

6.11**.** O Pregoeiro poderá encaminhar pelo sistema eletrônico contraproposta diretamente ao proponente que tenha apresentado o lance de menor preço, para que seja obtido preço melhor, bem como decidir sobre sua aceitação.

6.12**.** O sistema informará a proposta de menor preço (ou melhor proposta) imediatamente após o encerramento da etapa de lances ou, quando for o caso, após negociação e decisão pelo(a) pregoeiro acerca da aceitação do lance de menor valor.

6.13. Quando for constatado o empate, conforme estabelecem os artigos 44 e 45 da LC 123/2006, o(a) Pregoeiro aplicará os critérios para o desempate em favor da ME/EPP.

6.14. Constatando o atendimento das exigências fixadas no Edital, o objeto será adjudicado ao autor da proposta ou lance de menor preço.

7. DO JULGAMENTO

7.1. Para julgamento será adotado o critério de **menor preço**, observado o prazo para fornecimento, as especificações técnicas, parâmetros mínimos de desempenho e de qualidade e demais condições definidas neste Edital.

7.2. DO BENEFÍCIO ÀS MICROEMPRESAS E EMPRESAS DE PEQUENO PORTE QUANDO O ITEM/LOTE DO PREGÃO ELETRÔNICO NÃO FOR EXCLUSIVO PARA MICROEMPRESAS E EMPRESAS DE PEQUENO PORTE:

7.2.1. Encerrada a fase de lances, se a proposta de menor lance não tiver sido ofertada por microempresa ou empresa de pequeno porte e o sistema eletrônico identificar que houve proposta apresentada por microempresa ou empresa de pequeno porte igual ou até 5% (cinco por cento) superior à proposta de menor lance, será procedido o seguinte:

7.2.2. A microempresa ou empresa de pequeno porte mais bem classificada será convocada pelo sistema eletrônico, via "chat" de comunicação do pregão eletrônico, para, no prazo de 05 (cinco) minutos após a convocação, apresentar nova proposta inferior aquela considerada vencedora do certame, situação em que, atendidas as exigências habilitatórias, será adjudicado em seu favor o objeto do pregão;

7.2.3. No caso de empate de propostas apresentadas por microempresas ou empresas de pequeno porte que se enquadrem no limite estabelecido no subitem 7.2.1, o sistema realizará um sorteio eletrônico entre elas para que se identifique aquela que primeiro será convocada para apresentar melhor oferta, na forma do disposto na alínea "a";

7.2.4. Na hipótese da não contratação nos termos previstos no subitem 7.2.1, o objeto licitado será adjudicado em favor da proposta originalmente vencedora do certame, desde que atenda aos requisitos de habilitação.

7.3. O Pregoeiro anunciará o licitante detentor da melhor proposta ou lance de menor valor, imediatamente após o encerramento da etapa de lances da sessão pública ou, quando for o caso, após negociação e decisão pelo Pregoeiro acerca da aceitação do lance de menor valor.

7.4. Se a melhor proposta ou o lance de menor valor não for aceitável, o Pregoeiro examinará a proposta ou o lance subsequente, na ordem de classificação, verificando a sua aceitabilidade e procedendo à sua habilitação. Se for necessário, repetirá esse procedimento, sucessivamente, até a apuração de uma proposta ou lance que atenda ao Edital.

7.5. Da sessão, o sistema gerará ata circunstanciada, na qual estarão registrados todos os atos do procedimento e as ocorrências relevantes.

8. DAS IMPUGNAÇÕES E RECURSOS ADMINISTRATIVOS

8.1. Impugnação ou recursos administrativos devem ser dirigidos ao Pregoeiro somente pelo e-mail natanael.na@pmfi.pr.gov.br, no prazo legal ou protocolados no setor de protocolo geral do Município.

8.2. A intenção de interpor recurso na licitação deverá ser promovida através do Sistema Eletrônico, **após a declaração do vencedor** pelo Pregoeiro. A aceitação da intenção de recurso será feita pelo Sistema Eletrônico nas 24 (vinte e quatro) horas posteriores ao ato de declaração do vencedor, inclusive para os casos de empresas desclassificadas antes da fase de disputa.

8.3. Manifestada a intenção de interpor recurso, o recorrente terá o prazo máximo de 3 (três) dias úteis para apresentação de suas razões, ficando facultado aos demais licitantes a apresentação das contrarrazões do recurso, no mesmo prazo de 3 (três) dias úteis, cuja contagem iniciar-se-á a partir do término do prazo do recorrente, sendo-lhes assegurada vistas ao processo.

8.4. Não serão conhecidas as impugnações e os recursos apresentados fora do prazo legal e/ou subscritos por representantes não habilitados legalmente. A falta de manifestação imediata e motivada na forma estabelecida neste capítulo importará a preclusão do recurso e consequente adjudicação do objeto do certame aos licitantes vencedores.

8.5. Não será concedido prazo para recursos sobre assuntos meramente protelatórios ou quando não justificada a intenção de interpor o recurso pelo proponente.

8.6. Os recursos contra decisões do Pregoeiro **não** terão efeito suspensivo.

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

8.8. O Pregoeiro deverá encaminhar o recurso e suas contrarrazões à Autoridade Superior para decisão. A adjudicação do item objeto da licitação para os quais existirem recursos só poderá ser efetuada pela Autoridade Superior.

9. DA HOMOLOGAÇÃO

9.1 Encerrada a etapa de recursos o Pregoeiro deverá emitir o relatório do certame, indicando as ocorrências desde a sua abertura até o seu término, encaminhando-o à autoridade superior para decisão final.

9.2 A autoridade superior decidirá sobre a homologação do certame, retornando o relatório ao Pregoeiro, para continuidade do processo, na forma do edital.

10. DA FORMALIZAÇÃO DO INSTRUMENTO CONTRATUAL

10.1 O Contrato a ser firmado com a empresa vencedora incluirá as condições estabelecidas neste edital e em seus anexos, além de outras fixadas na proposta vencedora e necessárias à fiel execução do objeto licitado, conforme minuta de contrato anexa;

10.2 A prestação do(s) serviços(s) dar-se-á mediante contrato, a ser firmado entre o licitador e a proponente vencedora da licitação, após a homologação da licitação;

10.1. Adjudicado o objeto da presente licitação, a Prefeitura Municipal de Foz do Iguaçu convocará o adjudicado para assinar o termo de contrato ou aceitar outro instrumento hábil em até 5 (cinco) dias úteis, sob pena de decair o direito à contratação, sem prejuízo das sanções previstas no artigo 81 da Lei nº 8.666/93. Este prazo poderá ser prorrogado uma vez, quando solicitado pelo licitante vencedor durante o seu transcurso e desde que ocorra motivo justificado e aceito pelo Município de Foz do Iguaçu.

10.3 A Prefeitura Municipal de Foz do Iguaçu poderá, quando o convocado não assinar o contrato ou aceitar outro instrumento hábil no prazo e condições estabelecidos neste instrumento convocatório, convocar os proponentes remanescentes, na ordem de classificação, para fazê-lo em igual prazo e nas condições propostas pelo primeiro classificado, inclusive quanto aos preços, atualizados de conformidade com o presente edital, ou revogar a licitação, independentemente da cominação prevista no art. 81 da Lei nº 8.666/93.

10.4 Para fins de assinatura do contrato a licitante vencedora deverá apresentar Certidão Negativa de Débitos expedida pela Prefeitura Municipal de Foz do Iguaçu, em atendimento ao art. nº 178 do Código Tributário Municipal (LC nº 082/2003), se empresa sediada no Município de Foz do Iguaçu.

10.5 A contratada deverá manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação (art. 55, XIII da Lei 8.666/93).

11. FISCALIZAÇÃO E RECEBIMENTO DO SERVIÇO

11.1 A fiscalização da execução do(s) serviços(s) será feita por servidores devidamente credenciado pela Secretaria Municipal da Tecnologia da Informação, com responsabilidades específicas.

11.2 Serão designados os seguintes servidores para fiscalização e gestão do objeto contratual:

GESTOR do contrato:

- **Nome:** Evandro Ferreira

- **Cargo/Função:** Secretário Municipal de Tecnologia da Informação.

FISCAL do contrato:

- **Nome:** Sandro Lopes Ebbing;
- **Cargo/Função:** Diretor de Infraestrutura e Segurança da Informação.

12. DAS CONTRATAÇÕES E DAS SANÇÕES.

12.1 As contratações se darão através da formalização de Termo de Contrato.

12.2 O Instrumento Contratual deverá conter:

I - O objeto e seus elementos característicos, inclusive quantidades;
II - A forma e o prazo da prestação dos serviços;
III - O preço unitário e total;
IV - A indicação do respectivo processo licitatório.

12.3 Com fundamento no art. 7° da lei n° 10.520/2002, ficará impedida de licitar e contratar com quaisquer órgãos da União e com base no art. 87, inciso II da Lei 8.666/1993, estará sujeito á multa, de acordo com a gravidade do inadimplemento cometido, a empresa que:

12.3.1 Não mantiver sua proposta ou deixar de apresentar quaisquer documentos exigidos pelo edital de licitação:

a) Recusar-se ou deixar de enviar a documentação e a proposta de preços no prazo estabelecido no edital;
b) Recusar-se ou deixar de responder diligência realizada pela PMFI, durante a análise da proposta;
c) Deixar de manter as condições de habilitação;
d) Desistir expressamente de sua proposta, após a abertura da licitação, sem justificativa aceita pela Administração.

12.3.1.1 Para os casos correlatos a este item, a empresa inadimplente ficará impedida de licitar e *contratar com a Prefeitura do Município de Foz do Iguaçu, pelo prazo de 01 (ano) ano, além de multa de 3% (três por cento) em relação ao total de sua proposta.*

12.3.2 Deixar de celebrar o Contrato:

a) Recusar-se ou deixar de enviar documento (s) necessário (s) à comprovação de capacidade para assinatura do Contrato: *impedimento de licitar e contratar com a Prefeitura do Município de Foz do Iguaçu pelo prazo de 01 (um) ano e multa de 10% (dez por cento) em relação ao valor total de sua proposta*;

b) Recusar-se ou deixar de assinar o Contrato, dentro do prazo de validade da sua proposta: *Impedimento de licitar e contratar com a Prefeitura do Município de Foz do Iguaçu, pelo prazo de 01 (um) ano e multa de 10% (dez por cento) em relação ao valor total de sua proposta;*

12.3.3 Fraudar ou falhar na execução do Contrato, e ensejar retardamento de sua execução:

a) Pela inexecução parcial do Contrato: *aplicar as sanções previstas no artigo nº 87 da Lei nº 8.666/93, sendo que no caso de multa, esta corresponderá a 5% do valor da parcela inadimplida;*

b) Pela inexecução total do Contrato: *aplicar as sanções previstas no artigo nº 87 da Lei nº 8.666/93, sendo que no caso de multa esta corresponderá a 10% do valor contratual.*

c) Se a contratada ceder o Contrato, no todo ou em parte, a pessoa física ou jurídica, sem autorização do contratante, ainda que obrigada a reassumir a execução do(s) serviço(s) no prazo máximo de 15 (quinze) dias: *Multa de 10% (dez por cento) do valor contratual.*

a) Deixar de prestar a garantia prevista no item 13, dentro do prazo exigido pelo edital de licitação: *Multa de* 0,07% (sete centésimos por cento) do valor do contrato por dia de atraso, observado o máximo de 2% (dois por cento).

12.3.4 Apresentar documento ou declaração falsa:

a) Omitir informações em quaisquer documentos exigidos no certame licitatório: *Impedimento de licitar e contratar com quaisquer órgãos da Administração Municipal por período de 01 (um) ano*;

b) Adulterar documento, público ou participar, com o fim de prejudicar direito, criar obrigações ou alterar a verdade: *impedimento de licitar com a Administração Municipal por 05 (cinco) anos;*

12.3.4.1 As empresas enquadradas neste item ficarão, ainda, sujeitas à multa de 20% (vinte por cento) em relação ao valor total de sua proposta.

12.3.5 Cometer fraude fiscal:

a) Fazer declaração falsa sobre seu enquadramento fiscal;
b) Omitir informações em suas notas fiscais ou de outrem;
c) Falsificar ou alterar quaisquer Notas Fiscais.

12.3.5.1 Para os casos correlatos a este item, a empresa ficará impedida de licitar e contratar com a Prefeitura do Município de Foz do Iguaçu, sendo penalizado com a declaração de inidoneidade, que acarreta o impedimento de licitar com a União, Estados e Municípios, pelo prazo de 05 (cinco) anos;

12.3.5.2 As empresas enquadradas neste item ficarão, ainda sujeitas à multa de 20% (vinte por cento) em relação ao valor total de sua proposta.

12.3.6 Comportar-se de modo inidôneo:

a) Atos comprovadamente realizados com má-fé ou dolo;
b) Participação na licitação de empresa constituída com a finalidade de burlar penalidade aplicada anteriormente, a qual será constatada com a verificação dos quadros societários,

objetos sociais e/ou seus endereços, da empresa participante e da penalidade anteriormente.

12.3.6.1 Para os casos correlatos a este item, a empresa ficará impedida de licitar e contratar com a Prefeitura do Município de Foz do Iguaçu, pelo prazo de 05 (cinco) anos, além do pagamento de multa de 20% (vinte por cento) sobre o valor total de sua proposta ou do Contrato, conforme o caso.

12.3.7 Além do acima exposto, a adjudicatária se sujeita às sanções de advertência e multa, constantes nos artigos 86 e 87, da Lei n° 8.666/1993, aplicadas suplementarmente, pela inobservância das condições estabelecidas para o fornecimento ora contratado, da seguinte forma:

a) Advertência, nos casos de menor gravidade;

b) Multa de mora de 0,66% (*zero vírgula sessenta e seis por cento*) calculada sobre o total devido, por dia de atraso na entrega/prestação do serviço, objeto do Edital, sendo que a partir do 31° (trigésimo primeiro) dia de atraso, este será considerado como inexecução total do Contrato, incidindo sanções específicas, conforme item 12.3.1 "b" acima.

12.3.8 As sanções previstas nesta seção não impedem a Administração de exigir indenizações suplementares para reparar os danos advindos da violação de deveres contratuais, apurados durante o processo administrativo de penalização.

12.3.9 Será assegurada à empresa, previamente à aplicação das penalidades mencionadas nesta seção, o direito ao contraditório e à ampla defesa.

12.3.10 A aplicação de uma das penalidades previstas nesta seção não exclui a possibilidade de aplicação de outras.

12.3.11 As penalidades serão obrigatoriamente registradas no SICAF e, no caso de impedimento de licitar e contratar, o licitante será descredenciado por igual período, sem prejuízo das multas previstas no Edital, no contrato e das demais cominações legais.

12.3.12 A dosimetria das penas, além dos fatos e provas constantes do processo administrativo, levará em consideração:

a) O dano causado à administração;
b) O caráter educativo da pena;
c) A reincidência como maus antecedentes;
d) A proporcionalidade.

12.3.13 Ainda, nos casos em que couber, serão aplicadas as sanções previstas na Lei Federal 12.846/2013, que dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas ela prática de atos contra a administração pública, nacional ou estrangeira, e dá outras providências.

12.3.14 Caso as multas previstas no edital de licitação não sejam suficientes para indenizar os danos sofridos pela Administração, esta poderá cobrar, administrativa e judicialmente, os

prejuízos excedentes, tendo, neste caso, que provar os danos, conforme dispõe o art. 416 do Código Civil Brasileiro.

13. CLÁUSULA NONA - DA GARANTIA DE EXECUÇÃO

A CONTRATADA deverá apresentar à Administração, no prazo máximo de 10 (dez) dias úteis, contado da data da assinatura do Contrato, comprovante de prestação de garantia correspondente ao percentual de **5%** (**cinco por cento**) do valor do contrato, podendo essa optar por caução em dinheiro, títulos da dívida pública, seguro-garantia ou fiança bancária, com prazo de validade durante a execução do contrato e 3 (três) meses após o término da vigência contratual, devendo ser renovada a cada prorrogação.

A garantia assegurará, qualquer que seja a modalidade escolhida, o pagamento de:

a) Prejuízo advindo do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;
b) Prejuízos causados à administração ou a terceiro, decorrentes de culpa ou dolo durante a execução do contrato;
c) As multas moratórias e punitivas aplicadas pela Administração à contratada; e
d) Obrigações trabalhistas, fiscais e previdenciárias de qualquer natureza, não honradas pela contratada.

14. DO PAGAMENTO

14.1 O pagamento do objeto contratual será efetuado mensalmente em moeda brasileira corrente, em até 30 (trinta) dias após a apresentação correta da fatura dos serviços executados e medidos, além dos documentos pertinentes, devidamente protocolados, desde que cumpridas as cláusulas contratuais e obedecidas às condições para liberação das parcelas, observados o cronograma do Anexo I - Termo de Referência.

14.2 O faturamento deverá ser apresentado e protocolado, em uma via original, no protocolo geral na sede do CONTRATANTE;

14.3 O faturamento de cada parcela mensal deverá ser apresentado, conforme segue, de modo a padronizar condições e forma de apresentação:

14.3.1 Nota fiscal com discriminação resumida dos serviços executados, período de execução, número da licitação e termo de contrato de empreitada, não apresente rasura e/ou entrelinhas e esteja certificada pela Secretaria Municipal de Tecnologia da Informação;

14.4 É obrigatória a emissão de Nota Fiscal de Prestação de Serviços Eletrônica, na forma contida no Decreto Municipal nº 21.524 de 02 de Agosto de 2012, expedido em conformidade com a legislação federal (Protocolo ICMS 42/2009).

14.5 Para o recebimento dos pagamentos devidos, recomenda-se apresentar à Secretaria Municipal da Fazenda, os seguintes documentos para comprovação da regularidade fiscal:

14.5.1 Prova de regularidade relativa a Tributos Federais e à Divida Ativa da União, emitida conforme Portaria Conjunta RFB / PGFN nº.1.751 de 02/10/2014.

14.5.2 Prova de regularidade para com a Fazenda Estadual, mediante apresentação de Certidão Negativa de Débitos e Tributos Estaduais, expedida pela Secretaria de Estado da Fazenda, do domicílio ou sede da proponente;

14.5.3 Prova de regularidade para com a Fazenda Municipal, mediante apresentação de Certidão Negativa de Tributos Municipais, expedida pela Secretaria Municipal da Fazenda, do domicílio ou sede da proponente;

14.5.4 Prova de regularidade relativa ao Fundo de Garantia por Tempo de Serviços (FGTS), demonstrando situação regular no cumprimento dos encargos sociais instituídos por lei;

14.5.5 Prova de regularidade junto a Justiça do Trabalho, mediante a apresentação da Certidão Negativa de Débitos Trabalhistas, demonstrando a situação regular no cumprimento dos encargos trabalhistas instituídos por lei.

15. DISPOSIÇÕES FINAIS

15.1 O Município de Foz do Iguaçu poderá revogar a presente licitação, no todo ou em parte, por razões de interesse público derivadas de fato superveniente comprovado, ou anulá-la por ilegalidade, de ofício ou por provocação de terceiros, mediante ato escrito e fundamentado. O Município poderá, ainda, prorrogar, a qualquer tempo, os prazos para recebimento das propostas ou para sua abertura.

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

15.3 É facultado ao Pregoeiro, ou à autoridade a ele superior, em qualquer fase da licitação, promover diligências com vistas a esclarecer ou a complementar a instrução do processo. Os licitantes intimados para prestar quaisquer esclarecimentos adicionais deverão fazê-lo no prazo determinado pelo Pregoeiro, sob pena de desclassificação e/ou inabilitação.

15. 4 O desatendimento de exigências formais, não essenciais, não importará no afastamento do licitante, desde que seja possível a aferição da sua qualificação e a exata compreensão da sua proposta.

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

15.6 As decisões referentes a este processo licitatório poderão ser comunicadas aos licitantes por qualquer meio de comunicação que comprove o recebimento ou, ainda, mediante publicação no Órgão Oficial do Município.

15.7 Os casos não previstos neste Edital serão decididos pelo Pregoeiro.

15.8 A participação do licitante neste Pregão implica em aceitação de todos os termos deste Edital.

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

15.10 Quaisquer esclarecimentos serão formalizados por escrito através do endereço constante no preâmbulo deste Edital. As respostas serão postados no www.licitacoes-e.com.br para conhecimento de todos os interessados.

15.11 A documentação apresentada para fins de habilitação da empresa vencedora fará parte dos autos da licitação e não será devolvida ao proponente.

Os casos omissos serão resolvidos pelo Pregoeiro e, dependendo do caso, pela autoridade competente, nos termos da legislação pertinente. Para dirimir toda e qualquer dúvida e/ou divergência oriunda do presente Edital, será competente o Foro da Comarca de Foz do Iguaçu, Estado do Paraná.

Foz do Iguaçu, 28 de agosto de 2018.

Ney Patrício da Costa
Secretário Municipal da Administração

ANEXO I - TERMO DE REFERÊNCIA

1. IDENTIFICAÇÃO DO PROJETO

1.1. **Órgão Governamental Gestor:**

SECRETARIA MUNICIPAL DE TECNOLOGIA DA INFORMAÇÃO - SMTI.

1.2. **Título de Projeto:**

AQUISIÇÃO E IMPLEMENTAÇÃO DE SOLUÇÃO DE SEGURANÇA E CONECTIVIDADE DAS ÁREAS DE TECNOLOGIA DA INFORMAÇÃO DA PREFEITURA MUNICIPAL DE FOZ DO IGUAÇU – PARANÁ.

1.3. **Eixo estratégico:**

MODERNIZAÇÃO DAS ÁREAS DE TECNOLOGIA DA INFORMAÇÃO.

1.4. **Responsável legal:**

EVANDRO FERREIRA.

1.5. **Área responsável:**

SMTI / DIRETORIA DE INFRAESTRUTURA E SEGURANÇA DA INFORMAÇÃO.

1.6. **Equipe técnica responsável:**

Nome: SANDRO LOPES EBBING

Cargo/Função: DIRETOR DE INFRAESTRTURA E SEGURANÇA DA INFORMAÇÃO

Telefone: (45) 2105-1008 / 1007

1.7. **Data de elaboração do projeto:**

FEVEREIRO DE 2018.

2. DO OBJETO

Contratação de empresa especializada e tecnicamente qualificada para prestação dos serviços de fornecimento e implantação de solução de segurança e conectividade (*hardwares* - equipamentos e *softwares* - sistemas) para as áreas de tecnologia da informação da Prefeitura Municipal de Foz do Iguaçu, incluindo-se o fornecimento de equipamentos e sistemas necessários para a ampliação e/ou a substituição de ativos de rede, *internet*, *firewall*, *switches* e roteadores, bem como *softwares* e demais sistemas necessários, conforme descrição e quantitativos estabelecidos neste **Termo de Referência** e seus anexos.

3. CONTEXTUALIZAÇÃO (justificativa)

A Prefeitura Municipal de Foz do Iguaçu, através da Secretaria Municipal de Tecnologia da Informação, objetivando identificar e conhecer os gargalos e deficiências provocadas pela defasagem e obsolescência de *hardwares* (equipamentos) e *softwares* (sistemas) instalados e em operação tanto no *Data-Center* da SMTI como também nos demais setores da Prefeitura Municipal de Foz do Iguaçu, realizou amplo estudo de levantamento e coleta de dados e informações, verificação e testes, considerados relevantes para a tomada de decisão, em atendimento as demandas atuais e futuras, com vistas a aquisição e implementação de solução apropriada de segurança e conectividade para os ambientes (áreas) de Tecnologia da Informação da PMFI com vistas a modernizar e potencializar as ferramentas de trabalho da área

de Tecnologia da Informação que são disponibilizadas e utilizadas pelos usuários dos órgãos públicos municipais no desempenho de suas funções, atribuições e atividades relacionadas ao atendimento à população do município.

4. OBJETIVOS

O presente Termo de Referência buscará definir e orientar os procedimentos para contratação de empresa especializada e qualificada para prestação dos serviços de fornecimento e implantação de solução de segurança e conectividade para as áreas de tecnologia da informação da Prefeitura Municipal de Foz do Iguaçu que, atualmente, encontra-se obsoleta e defasada, oferecendo insegurança e ineficiência nos serviços de segurança da informação, acesso à internet, intranet e e-mails, objetivando modernizar e reestruturar o *Data-Center* primário da PMFI, instalado no prédio sede da SMTI, no que concerne a *hardwares e softwares*, bem como as demais estruturas e ambientes de T. I. da PMFI, proporcionando assim, aos seus usuários, melhores e adequadas condições para o desempenho e desenvolvimento de suas atividades relacionadas ao atendimento ao cidadão, maximizando e otimizando os recursos públicos disponíveis.

5. DA DOTAÇÃO ORÇAMENTÁRIA

5.1. Os recursos para a execução da despesa proveniente do presente Termo de Referência correrão à conta dos recursos alocados no orçamento do Município de Foz do Iguaçu, no Programa de Trabalho:

12.01.12.361.0120.1030.449052.3500.1.104; 12.03.12.361.0600.2114.339039.9400.1.103;
14.02.04.126.0140.1040.449052.3500.1.505; 14.02.04.126.0140.1040.339039.9400.1.505;
10.01.10.122.0100.2090.339039.9400.1.000; 10.01.10.122.0100.2090.449052.3500.1.303;
08.05.08.244.0080.1016.449052.3500.1.505; 08.05.08.244.0510.1015.449052.3500.1.505.

6. DO PRAZO PARA ENTREGA

6.1. Plano de trabalho (cronograma de implantação da solução completa):

6.1.1. Macro Plano de Implantação - REDE E SEGURANÇA

6.1.1.1. **Fase O:**

a) Survey e Premissas.

6.1.1.2. **Fase I:**

a) Todos os dispositivos serão instalados/cabeados ao lado/próximos dos mesmos dispositivos que irão substituir;
b) Os novos roteadores de borda Internet/Switches/Firewalls serão interconectados e seu funcionamento verificado;
c) Os switches abaixo dos novos firewalls/Web Proxy também serão configurados e ativados.
NOTA: Até esse momento nenhum tráfego de "produção" passará por esses dispositivos, apenas o tráfego de gerência (SNMP, SSH, etc.).

6.1.1.3. **Fase II:**

a) Migração:
- Será migrada a borda internet para os novos roteadores, mas o roteamento para o core continuará pelo firewall antiga;

- O tráfego da borda internet (já nos novos roteadores de borda) será desviado para os firewalls novos, a topologia abaixo dos firewalls permanecerá a mesma.

b) Ativação do Web Proxy:
- Testes manuais de proxy e caching serão realizados, os firewalls continuam permitindo a saída/chegada Web;
- Via GPO a estações serão obrigadas a ir para o Proxy;
- O tráfego Web será bloqueado nos firewalls e será permitido somente via o Proxy.

c) Configuração da solução EndPoint
- Instalação servidor;
- Configuração estações.

6.1.1.4. **Fase III:**

a) Migração dos switches de distribuição:
- Migração progressiva de cada secretaria para os novos switches;
- Desativar antigos switches.

b) Alteração de Topologia Lógica:
- Default gateway de cada secretaria para os firewalls/Novo plano de VLANs/Endereçamento;
- Remoção do cascateamento de switches em cada secretaria;
- Configuração de novas regras de proteção entre as secretarias (no firewall).

7. DAS CONDIÇÕES DE FORNECIMENTO

7.1. A CONTRATADA deverá prestar à CONTRATANTE os serviços de fornecimento e implantação de solução para segurança e conectividade das áreas de Tecnologia da Informação (*hardwares* – equipamentos e *softwares* – sistemas) da Prefeitura Municipal de Foz do Iguaçu, incluindo-se o fornecimento de equipamentos e sistemas necessários para a ampliação e/ou a substituição de ativos de rede, *internet*, *firewall*, *switches* e roteadores, bem como *softwares* e demais sistemas necessários, conforme descrição e quantitativos estabelecidos neste **Termo de Referência** e seus anexos.;

7.2. A CONTRATADA ficará obrigada a atender todas as exigências e especificações contidas neste Termo de Referência e seus anexos, bem como nas demais clausulas descritas no Edital de Licitação;

7.3. O contrato para prestação dos serviços descritos neste Termo de Referência só estará caracterizado mediante a:

7.3.1. Assinatura do contrato por ambas as partes;

7.3.2. Emissão, pela CONTRATANTE, da Nota de Empenho e recebimento pela CONTRATADA;

7.3.3. Emissão, pela CONTRATANTE, da ordem de serviços e recebimento pela CONTRATADA.

7.4. A CONTRATADA deverá, no ato da entrega e ativação dos serviços e equipamentos, fornecer documentos de garantia;

7.5. A PMFI/SMTI – Secretaria Municipal de Tecnologia da Informação será o órgão responsável pela gestão e fiscalização do contrato oriundo deste processo licitatório, bem como da execução dos serviços;

7.6. O acompanhamento e a fiscalização da execução do contrato consistem na verificação da conformidade da prestação dos serviços, de forma a assegurar o perfeito cumprimento do ajuste, devendo ser exercido por um ou mais representantes da PMFI – Prefeitura Municipal de Foz do Iguaçu, especialmente designados, na forma dos artigos 67 e 73 da Lei nº 8.666/1993, e do artigo 6º do Decreto nº 2.271/1997;

7.7. O descumprimento total ou parcial das demais obrigações e responsabilidades assumidas pela CONTRATADA ensejará a aplicação de sanções administrativas, previstas neste Termo de Referência e na legislação vigente, podendo culminar em rescisão contratual, conforme disposto nos artigos 77 e 80 da Lei nº 8.666/1993;

7.8. Para a emissão da **Nota de Empenho** será exigida a comprovação das condições de habilitação consignadas no edital, as quais deverão ser mantidas pelo licitante durante a vigência do contrato;

7.9. Quando o vencedor da licitação não fizer a comprovação referida no parágrafo anterior, ou quando injustificadamente recusar-se a cumprir o empenho, prazo e condições estabelecidas no ato convocatório da licitação, a PMFI, poderá convocar outro licitante, segundo a ordem de classificação, para, após a comprovação dos requisitos habilitatórios e feita a negociação, assinar o contrato, sem prejuízo das multas e demais cominações legais;

7.10. Os serviços a serem executados pela CONTRATADA serão fiscalizados e supervisionados pela Secretaria Municipal de Tecnologia da Informação da Prefeitura Municipal de Foz do Iguaçu – PR., a partir de agora denominada **SMTI**. Nos descritivos abaixo estarão especificados e detalhados todos os equipamentos e serviços, que compõem a solução de segurança e conectividade das áreas de T. I. pretendida pela PMFI, à serem instalados e implementados, bem como as suas fases de implantação e instalação e os objetivos a serem alcançados;

7.11. A CONTRATADA deverá fornecer ao corpo técnico da Prefeitura de Foz do Iguaçu o Projeto de Implementação, onde deverão constar procedimentos de validação para cada fase de implantação, seguindo as melhores práticas do fabricante e recomendando ações para correção de possíveis inconformidades, bem como Cronograma detalhado de Atividades. O cronograma detalhado deverá ser aprovado em comum acordo entre a LICITADA e a LICITANTE.

8. DAS DESCRIÇÕES, CARACTERISTICAS E ESPECIFICAÇÕES TÉCNICAS DE EQUIPAMENTOS E SERVIÇOS

8.1. QUANTIDADES:

TABELA DE ITENS A SEREM ADQUIRIDOS E CONTRATADOS (Segurança e Conectividade)		
ITEM	**Descrição**	**Qtd**
1	Firewall de Nova Geração – Firewall NGFW	2
2	Solução de Gerencia e Relatórios para Firewall NGFW	1

3	Switches tipo 1 (agregador)	4
4	Switches tipo 2 (core)	2
5	Solução de Email Gateway (appliance físico)	1
6	Solução de Segurança Web (appliance físico)	1
7	Roteador de Borda Internet Multi-Serviço	2
8	Solução Endpoint Security (número de dispositivos)	2.000
9	Expansão Storage EVA 4400	1
10	Consultoria Especializada **Security** N2 e N3	1
11	Consultoria Especializada **Routing and Switching** N2 e N3	1
12	Consultoria Especializada **VMWARE**	1
13	Treinamentos Oficiais – Categorias (4 alunos por categoria)	5

8.2. **Dispositivos Físicos Citados neste Termo de Referência:**

8.2.1. O equipamento deve de possuir um tempo médio entre falhas de, no mínimo, 180.000 horas;

8.2.2. O equipamento deverá estar em produção. Não serão aceitos modelos com End Of Sales, End Of Life e End of Support já anunciados pelo fabricante.

8.2.3. Todos equipamentos deverão ser novos, sem uso.

8.2.4. Não serão aceitas soluções baseadas em Open Source ou Codigo Livre.

8.2.5. Não serão aceitas licenças DEMO;

8.2.6. É indispensável a apresentação de Marca/Fabricante e Modelo;

8.2.7. Cada solução deverá ser composta por hardware e software do mesmo fabricante;

8.2.8. O fabricante do equipamento deve comprovar que dispõe de site publicamente acessível (via browser HTTP), nos quais disponibilizem versões atualizadas de firmware/software, informações técnicas e garantia do equipamento;

8.2.9. Todas as especificações devem ser comprovadas através de documentação dos respectivos fabricantes (manual original ou página do fabricante na INTERNET);

8.2.10. Onde aplicável os equipamentos devem operar em 127/240v automaticamente e o cabeamento elétrico deve usar o novo padrão brasileiro (NBR 14136 três pinos);

8.2.11. Os equipamentos devem ser fornecidos com documentação técnica e manuais que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização do equipamento. Deverá ser fornecido cabo console;

8.2.12. No ato do recebimento, será feita a conferência individual do(s) equipamento(s), que deverá(ão) conter a última versão pública de firmware/software;

8.2.13. As licitantes deverão comprovar a sua qualificação para o cumprimento do(s) objeto(s) desta licitação através de "Atestado de Capacidade Técnica", emitido por pessoa jurídica de direito público ou privado comprovando que a licitante forneceu equipamento de características e quantitativos semelhantes aos especificados no edital;

8.2.14. Garantia de um (01) ano da seguinte forma:

8.2.14.1. Os serviços de suporte e manutenção deste item deverão ser realizados em regime 8x5xNBD on site (8 horas x 5 dias da semana com prazo para resolução do problema até o dia útil subsequente à abertura do chamado técnico) pelo prazo mínimo de 01 (um) ano;

8.2.14.2. A contratante poderá abrir chamados de manutenção diretamente no fabricante do item, através de chamada gratuita a número 0800, com atendimento em português, ou por interface web, sem necessidade de prévia consulta e/ou qualquer liberação por parte da contratada. Não deve haver limite para aberturas de chamados, sejam de dúvidas/configurações e/ou resolução de problemas de hardware ou software. Poderá ser solicitado ao fabricante acesso remoto aos equipamentos para ajuda na correção de problemas dos diversos tipos inclusive configuração sem custos adicionais ou necessidade de autorização da contratada no momento desta abertura;

8.2.14.3. Deverá ser garantido à contratante o pleno acesso ao site do fabricante dos equipamentos e softwares. Esse acesso deve permitir consultas a quaisquer bases de dados disponíveis para usuários relacionadas aos equipamentos e softwares especificados, além de permitir downloads de quaisquer atualizações de software ou documentação deste produto.

8.2.15. A proposta deve incluir as horas para instalação, configuração inicial, burn-in, testes, migração das configurações existentes para os novos equipamentos, cabeamento, bastidores adicionais se necessários (compatíveis com os já existentes na PMFI), sugestões de design, documentações (LLD, HLD, Planos de Trabalho, etc.), inserção dos equipamentos no sistema de gerência da PMFI, acompanhamento on site e remoto nas primeiras 48 horas contadas a partir da entrada em produção dos equipamentos. Relatórios finais devem ser entregues juntamente com o HLD/LLD para o aceite final da implantação assinado por profissionais com a mais alta qualificação técnica do fabricante para cada uma das tecnologias/soluções oferecidas. Os documentos também devem ser entregues assinados por um profissional com qualificação ITIL e PMI. Todas as configurações devem seguir as mais recentes BCP para cada tipo de dispositivo/função ofertada. Será dada oportunidade aos proponentes para um site-survey nas dependências da PMFI bem como perguntas adicionais por escrito referente a esse item;

8.2.16. No momento da entrega da documentação supracitada todos os assinantes devem fazer parte do quadro da empresa e estarem na mesma por pelo menos dois anos;

8.2.17. A instalação/configuração deverá ser feita por pessoal qualificado pelo fabricante para realizar tal tarefa e os executores deverão ser funcionários da proponente/vencedora do processo licitatório. Em nenhuma hipótese deverá ser realizada por terceiros;

8.2.18. As atividades de implantação, configuração, migração considerando-se tratar-se de uma rede em produção poderão se estender por até 3 meses após a assinatura do contrato.

8.3. **Itens Virtualizados, Softwares de Gerência, Solução de Endpoint Security:**

8.3.1. A solução deverá estar em produção. Não serão aceitas soluções descontinuadas nem que estejam anunciados para serem descontinuados pelo FABRICANTE;

8.3.2. É indispensável a apresentação de Marca/FABRICANTE e Versão;

8.3.3. A solução deverá ser composta por software de um único fabricante;

8.3.4. O FABRICANTE da solução deve comprovar que dispõe de site publicamente acessível (via browser HTTP), nos quais disponibilizem versões atualizadas de firmware/software, informações técnicas e garantia da solução ofertada;

8.3.5. Todas as especificações devem ser comprovadas através de documentação dos respectivos FABRICANTES (manual original ou página do FABRICANTE na INTERNET);

8.3.6. A solução deve ser fornecida com documentação técnica e manuais que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização da solução;

8.3.7. No ato do recebimento, será feita a conferência individual dos itens, que deverão conter a última versão pública de firmware/software;

8.3.8. As licitantes deverão comprovar a sua qualificação para o cumprimento do(s) objeto(s) desta licitação através de "Atestado de Capacidade Técnica", emitido por pessoa jurídica de direito público ou privado comprovando que a licitante forneceu equipamento de características e quantitativos semelhantes aos especificados neste Termo de Referência.

8.4. **GARANTIA E SUPORTE TÉCNICO:**

8.4.1. **CANAIS DE ATENDIMENTO:**

8.4.1.1. Atendimento deverá ser feito através de canal telefônico gratuito 0800 e por meio de endereço WEB ou outro meio similar. Os canais de atendimento deverão ser informados quando da assinatura do contrato;

8.4.1.2. Os canais de atendimento deverão estar disponíveis 10 (dez) horas por dia (das 08h às 18h em horário de Brasília), 5 (cinco) dias por semana (de segunda-feira à sexta-feira);

8.4.1.3. O atendimento será realizado em Língua Portuguesa em primeiro nível, facultando-se o uso da Língua Inglesa nos demais níveis.

8.4.2. **SOLUÇÃO OFERTADA:**

8.4.2.1. Deverá ser ofertada garantia compreendendo suporte técnico a todos os componentes da solução ofertada, prestados pelo FABRICANTE de cada componente, por um período de 12 (doze) meses a contar da data de aceite;

8.4.2.2. O suporte técnico ofertado se dará em ambiente de produção e compreenderá a assistência na instalação, testes de aplicativo, uso, diagnóstico e solução de problemas e correções de bugs em softwares empacotado na distribuição suportada;

8.4.2.3. Durante o período de garantia, deverão ser disponibilizados, sem quaisquer ônus adicionais à CONTRATANTE, atualizações *patches* corretivas e novas versões dos produtos que integram a solução adquirida.

8.4.3. **Chamados, Registros e Início de Prazos:**

8.4.3.1. Será aberto um chamado técnico para cada problema reportado;

8.4.3.2. Os prazos para atendimento aos chamados de qualquer severidade serão considerados a partir da hora em que o chamado é aberto, isto é, registrado no canal disponibilizado pelo fabricante, recebendo dele uma identificação para acompanhamento, controle e histórico.

8.4.4. **Manutenções:**

8.4.4.1. Deverão ser providas, sempre que necessárias, as correções e/ou atualizações da solução disponibilizada, que garantam compatibilidade com os demais componentes de hardware e software da CONTRATANTE, sem ônus adicional para a mesma;

8.4.4.2. No caso de manutenções, preventivas ou corretivas, em que haja risco de indisponibilidade total ou parcial do ambiente computacional, a CONTRATANTE deverá ser previamente notificada para que se proceda à aprovação e o agendamento da manutenção em horário conveniente;

8.4.4.3. A instalação/configuração deverá ser feita por pessoal qualificado pelo fabricante para realizar tal tarefa e os executores deverão ser funcionários da proponente/vencedora deste processo licitatório. Em nenhuma hipótese deverá ser realizada por terceiros;

8.4.4.4. As atividades de implantação, configuração, migração considerando-se tratar-se de uma rede em produção poderão se estender por até 3 meses após a assinatura do contrato.

8.5. **FIREWALL DE PRÓXIMA GERAÇÃO (NEXT GENERATION FIREWALL - NGFW):**

8.5.1. **CARACTERÍSTICAS GERAIS:**

8.5.1.1. O equipamento de Firewall deve possuir as capacidades e características abaixo:

8.5.1.2. **CARACTERÍSTICAS DE HARDWARE FIREWALL :**

8.5.1.2.1. Deve possuir capacidade de processamento de, no mínimo, 3 (três) Gbps para tráfego stateful inspection multiprotocolo com a funcionalidade de firewall e controle de aplicações ativas simultaneamente, considerando-se para fins de métrica ambientes de produção;

8.5.1.2.2. Deve possuir capacidade de processamento de, no mínimo, 3 (tres) Gbps para tráfego stateful inspection multiprotocolo com a funcionalidade de firewall, controle de aplicações e IPS ativas simultaneamente, considerando-se para fins de métrica ambientes de produção;

8.5.1.2.3. O Firewall NGFW deve ser do tipo Appliance, com hardware e software desenvolvidos e fornecidos pelo mesmo fabricante com máximo de 1U de altura e padrão rack 19".

8.5.1.2.4. Não serão aceitos equipamentos servidores de uso genérico;

8.5.1.2.5. Deve possuir capacidade de processamento de, no mínimo, 2.5 (dois e meio) Gbps para tráfego stateful inspection multiprotocolo com a funcionalidade de firewall, controle de aplicações, IPS e Prevenção contra agentes maliciosos persistentes (Anti-Malware) ativas simultaneamente, considerando-se para fins de métrica ambientes de produção;

8.5.1.2.6. Deve possuir capacidade de throughput mínimo de 1Gbps para IPSEC VPN com pacotes TCP 1024Bytes.

8.5.1.2.7. Suporte a, no mínimo, 1.000.000 (um milhão) de conexões simultâneas;

8.5.1.2.8. Suporte a, no mínimo, 15.000 (quinze mil) novas conexões por segundo;

8.5.1.2.9. Possuir pelo menos 12 (doze) interfaces de rede 1 Gbps RJ-45 habilitadas para uso;

8.5.1.2.10. Além das 12 interfaces da configuração mínima, permitir acrescentar até 4 (quatro) interfaces de rede 1 Gbps SFP ;

8.5.1.2.11. Deve possuir 1 (uma) interface de rede Gigabit dedicada para gerenciamento;

8.5.1.2.12. Deve possuir 1 (uma) interface do tipo console ou similar;

8.5.1.2.13. Disco de, no mínimo, 100(cem)GB para armazenamento de informações locais.

8.5.1.3. **CARACTERÍSTICAS GERAIS DO FIREWALL:**

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

8.5.1.3.2. Deve estar operacional e licenciado sem restrições por 12 meses para todas as features de NGFW: URL Filtering, NGIPS e Proteção contra ameaças avançadas com cloud Sandboxing;

8.5.1.3.3. 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;

8.5.1.3.4. Deverá ser possível acessar o equipamento para aplicar configurações durante momentos onde o trafego é muito alto e a CPU e memória do equipamento estiverem com alto nível de utilização através de isolamento do processamento de gerenciamento e do processamento do tráfego inspecionado;

8.5.1.3.5. Por cada equipamento que compõe a plataforma de segurança, entende-se o hardware e as licenças de softwares necessárias para o seu funcionamento;

8.5.1.3.6. Na data da proposta, nenhum dos modelos ofertados poderá estar listados no site do fabricante em listas de end-of-life e end-of-sale;

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

8.5.1.3.8. O software deverá ser fornecido em sua versão mais recente e atualizado;

8.5.1.3.9. O acesso via SSH, cliente ou WEB (HTTPS); gerenciamento da solução deve suportar

8.5.1.3.10. Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:

8.5.1.3.10.1. Suporte a 1024 VLAN Tags 802.1q;

8.5.1.3.10.2. Agregação de links 802.3ad e LACP;

8.5.1.3.10.3. DHCP Relay;

8.5.1.3.10.4. DHCP Server;

8.5.1.3.10.5. Jumbo Frames;

8.5.1.3.10.6. Suportar sub-interfaces ethernet lógicas;

8.5.1.3.10.7. Deve suportar os seguintes tipos de NAT:

8.5.1.3.10.7.1. NAT dinâmico (Many-to-1);

8.5.1.3.10.7.2. NAT dinâmico (Many-to-Many);

8.5.1.3.10.7.3. NAT estático (1-to-1);

8.5.1.3.10.7.4. NAT estático (Many-to-Many);

8.5.1.3.10.7.5. NAT estático bidirecional 1-to-1;

8.5.1.3.10.7.6. Tradução de porta (PAT);

8.5.1.3.10.7.7. NAT de Origem;

8.5.1.3.10.7.8. NAT de Destino;

8.5.1.3.10.7.9. Suportar NAT de Origem e NAT de Destino simultaneamente;

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

8.5.1.3.10.7.11. NAT64 e NAT46.

8.5.1.3.11. Deve permitir monitorar via SNMP falhas de hardware, uso de recursos e estatísticas de uso das interfaces de rede;

8.5.1.3.12. Enviar log para sistemas de monitoração externos, simultaneamente;

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

8.5.1.3.14. Proteção contra anti-spoofing;

8.5.1.3.15. Implementar otimização do tráfego entre dois equipamentos;

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

8.5.1.3.17. Para IPv6, deve suportar roteamento estático e dinâmico ;

8.5.1.3.18. 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);

8.5.1.3.19. Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;

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

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

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

8.5.1.3.23. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo;

8.5.1.3.24. Em modo transparente;

8.5.1.3.25. Em layer 3;

8.5.1.3.26. A configuração em alta disponibilidade deve sincronizar:

8.5.1.3.26.1. Sessões;

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

8.5.1.3.26.3. Associações de Segurança das VPNs.

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

8.5.1.3.28. A configuração em alta disponibilidade deve possibilitar a instalação de cada membro do cluster, de forma que o

sincronismo de sessões e configurações deve ocorrer sobre a camada 3 (IP)

8.5.1.3.29. As características descritas deverão ser passíveis de comprovação por meio de documentação acessível no site do fabricante na Internet.

8.5.2. **CONTROLE POR POLÍTICA DE FIREWALL:**

8.5.2.1. Deverá suportar controles por zona de segurança;

8.5.2.2. Controles de políticas por porta e protocolo;

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

8.5.2.4. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;

8.5.2.5. Controle de políticas por País (geolocation);

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

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

8.5.2.8. Deve de-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.2;

8.5.2.9. Bloqueios dos seguintes tipos de arquivos: bat, cab, dll, exe, bin, zip, tar e mp3;

8.5.2.10. Suporte a objetos e regras IPV6;

8.5.2.11. Suporte a objetos e regras multicast;

8.5.2.12. Deve suportar no mínimo os seguintes tipos de negação de tráfego nas políticas de firewall: Drop sem notificação do bloqueio ao usuário, Drop com notificação do bloqueio ao usuário, TCP-Reset para o client, TCP-Reset para o server ou para os dois lados da conexão.

8.5.3. **CONTROLE DE APLICAÇÕES:**

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

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

8.5.3.3. Reconhecer pelo menos 1700 (Hum mil e setecentas) 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;

8.5.3.4. 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, webex , google-docs;

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

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

8.5.3.7. 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;

8.5.3.8. 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;

8.5.3.9. 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;

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

8.5.3.11. Atualizar a base de assinaturas de aplicações automaticamente;

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

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

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

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

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

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

8.5.3.18. 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;

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

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

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

8.5.3.22. Deve possibilitar a diferenciação de tráfegos Peer2Peer (ex.:Bittorrent, emule, neonet) possuindo granularidade de controle/políticas para os mesmos;

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

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

8.5.4. **PREVENÇÃO DE AMEAÇAS:**

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

8.5.4.2. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos;

8.5.4.3. Deve sincronizar as assinaturas de IPS quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;

8.5.4.4. 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;

8.5.4.5. Deve permitir ativar, desativar e habilitar apenas em modo de monitoração as assinaturas de prevenção contra invasão;

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

8.5.4.7. Deve suportar granularidade nas políticas de IPS, possibilitando a criação de diferentes politicas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens:

8.5.4.7.1. Deve permitir o bloqueio de vulnerabilidades;

8.5.4.7.2. Deve permitir o bloqueio de exploits conhecidos;

8.5.4.7.3. Deve incluir proteção contra ataques de negação de serviços;

8.5.4.7.4. Deverá possuir os seguintes mecanismos de inspeção de IPS:

8.5.4.7.4.1. Análise de padrões de estado de conexões;

8.5.4.7.4.2. Análise de decodificação de protocolo;

8.5.4.7.4.3. Análise para detecção de anomalias de protocolo;

8.5.4.7.4.4. Análise heurística;

8.5.4.7.4.5. IP Defragmentation;

8.5.4.7.4.6. Remontagem de pacotes de TCP;

8.5.4.7.4.7. Bloqueio de pacotes malformados;

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

8.5.4.7.4.9. Detectar e bloquear a origem de portscans;

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

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

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

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

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

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

8.5.4.7.9. Suportar bloqueio de arquivos por tipo;

8.5.4.7.10. Identificar e bloquear comunicação com botnets;

8.5.4.7.11. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:

8.5.4.7.12. O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;

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

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

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

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

8.5.4.7.17. Deve permitir a análise do comportamento da rede fornecendo visibilidade do uso do segmento monitorado para auxiliar na solução de falhas de rede ou degradação de desempenho, no mínimo as seguintes informações devem ser disponibilizadas:

8.5.4.7.17.1. Fluxos de sessão dos hosts;

8.5.4.7.17.2. Hora de início/fim;

8.5.4.7.17.3. Quantidade de dados trafegados.

8.5.4.7.18. Deve permitir coletar, armazenar e correlacionar as informações adquiridas passivamente, sobre hosts que trafegam pelos segmentos monitorados pelo (s) IPS. No mínimo as seguintes informações devem ser correlacionadas e armazenadas:

8.5.4.7.18.1. Sistema operacional do Host;

8.5.4.7.18.2. Serviços existentes no Host;

8.5.4.7.18.3. Portas em uso no Host;

8.5.4.7.18.4. Aplicações em uso no Host;

8.5.4.7.18.5. Vulnerabilidades existentes no Host;

8.5.4.7.18.6. Smart phones e tablets;

8.5.4.7.18.7. Network flow;

8.5.4.7.18.8. Anomalias de redes;

8.5.4.7.18.9. Identidades de usuários;

8.5.4.7.18.10. Tipo de arquivo e protocolo;

8.5.4.7.18.11. Conexões maliciosas.

8.5.4.7.19. Deve permitir criar uma lista com o ”ambiente ideal esperado” e a cada mudança nesse ambiente, o sensor de IPS deverá no mínimo alertar a console de gerencia sobre a mudança identificada. Entendemos como “ambiente ideal esperado” o conjunto de informações pré- configuradas na gerencia dos sensores de IPS a respeito dos atributos dos hosts participantes desse segmento, deve sercapaz de identificar no mínimo os seguintes atributos:

8.5.4.7.19.1. Sistema Operacional;

8.5.4.7.19.2. Serviços vigentes nos hosts;

8.5.4.7.19.3. Aplicações autorizadas a serem executadas nos hosts;

8.5.4.7.19.4. Aplicações não autorizadas a serem executadas nos hosts.

8.5.4.7.20. Proteção contra downloads involuntários usando HTTP de arquivos executáveis, maliciosos;

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

8.5.5. **ANÁLISE DE MALWARES MODERNOS:**

8.5.5.1. Devido aos Malwares hoje em dia serem muito dinâmicos e um antivírus comum reativo não ser capaz de detectar os mesmos com a mesma velocidade que suas variações são criadas, a solução ofertada dever possuir funcionalidades para análise de Malwares não conhecidos incluídas na própria ferramenta ou entregue com composição com outro fabricante;

8.5.5.2. O dispositivo de proteção deve ser composto por equipamento tipo appliance especializado na proteção em tempo-real contra Ameaças Avançadas, Persistentes e ataques direcionados em tráfego de Internet ou local;

8.5.5.3. Deve suportar operação em ambientes configurados para alta disponibilidade;

8.5.5.4. O dispositivo de proteção deve ser capaz de enviar arquivos trafegados de forma automática para análise "*In Cloud*" ou local, onde o arquivo será executado e simulado em ambiente controlado;

8.5.5.5. Deve permitir de forma automática a criação e manutenção de um histórico ou fluxo de trabalho forense no qual seja possível identificar:

8.5.5.5.1. Inserção de malware no ambiente de rede, movimento lateral, mesmo quando esta não seja detectada inicialmente como malware.

8.5.5.5.2. Identificar e acompanhar em tempo-real atividades de criação, movimento, execução de arquivos e processos, mesmo quando não sejam detectados ou conhecidos como maliciosos;

8.5.5.5.3. Permitir as condições dos pontos anteriores em múltiplos ativos monitorados no ambiente de forma simultânea e automatizada.

8.5.5.6. Deve permitir selecionar através de políticas granulares quais tipos de arquivos sofrerão esta análise incluindo, mas não limitado a: endereço IP de origem/destino, usuário/grupo do AD/LDAP, aplicação, porta, URL/categoria de URL de destino, tipo de arquivo e todas estas opções simultaneamente;

8.5.5.7. Suportar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, os seguintes sistemas operacionais, Windows X (32 e 64 bits);

8.5.5.8. Deve suportar a monitoração, detecção e prevenção em tempo real de arquivos trafegados nos seguintes protocolos HTTPS, FTP, HTTP, SMTP, IMAP, POP3 como também arquivos trafegados internamente entre servidores de arquivos usando SMB em todos os modos de implementação: sniffer, transparente e L3;

8.5.5.9. O sistema de análise "*In Cloud*" ou local deve prover informações sobre as ações do Malware na máquina infectada, informações sobre quais aplicações são utilizadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo Malware, definir URLs não confiáveis utilizadas pelo novo Malware e prover informações sobre o usuário infectado (seu endereço ip e seu login de rede);

8.5.5.10. Deve permitir especificar o tipo de arquivo, inclusive os comprimidos que serão analisados em cada política de controle de malware, permitindo especificar um contexto de análise para redes, vlans e outros objetos associados ao controle de acesso do ambiente protegido;

8.5.5.11. Permitir que seja definido o tamanho máximo dos arquivos a serem inspecionados;

8.5.5.12. Deve utilizar mecanismo de proteção baseado em reputação global em tempo-real, permitindo assim que sejam adotadas ações automáticas de alerta e bloqueio de arquivos suspeitos ou malwares já encontrados anteriormente;

8.5.5.13. O dispositivo não deve depender ou utilizar de forma exclusiva mecanismos de análise em ambiente virtualizado para que seja feita a detecção e o bloqueio de ameaças malwares em tempo-real;

8.5.5.14. A utilização de recursos de execução virtualizada, não deve depender da configuração manual de imagens ou escolha de versões específicas de sistemas operacionais;

8.5.5.15. Deve possuir mecanismo blacklist para implementar controles customizados de forma automatizada;

8.5.5.16. Deve possuir mecanismo whitelist para implementar controles customizados de forma automatizada;

8.5.5.17. Deve possuir capacidade para detecção de Malwares em comunicações de entrada e saída, incluindo a detecção de mecanismos de Comando e Control.

8.5.5.18. Deve possuir capacidade de execução de amostras tipo arquivos executáveis em ambiente Windows virtualizado, permitindo a análise completa do comportamento com ou sem utilização de assinaturas para identificar o nível de ameaça da amostra;

8.5.5.19. Deve identificar ataques como: ataques direcionados, Zero Day, exploração de vulnerabilidades, indicadores de obfuscação e indicadores de comprometimento automáticos;

8.5.5.20. Deve possuir tecnologia proprietária de execução para verificação de Malwares avançados inclusive mecanismos tipo sandbox;

8.5.5.21. O dispositivo deve ser capaz de atingir níveis elevados de detecção (exemplo condições de ataques dia-zero) com prevenção em tempo real mesmo em caso de falha ou parada total do recurso de análise virtualizado (sandbox);

8.5.5.22. Deve implementar a identificação e capacidade de controle de acesso em tempo real nos seguintes tipos de arquivo: MSEXE, 9XHIVE, DMG, DMP,ISO,NTHIVE,PCAP,PGD,SYLKc,SYMANTEC,VMDK,DWG,IMG_PICT,MAYA,

PSD,WMF,SCRENC,UUENCODED,PDF,EPS,AUTORUN,BINARY_DATA,BINHEX, EICAR, ELF,ISHIELD_MSI, MACHO, RPM, TORRENT, AMR, FFMPEG, FLAC, FLIC, FLV, IVR, MIDI, MKV,MOV,MPEG,OGG,PLS,R1M,REC,RIFF,RIFX,RMF,S3M,SAMI,SMIL,SWF,WAV,WEBM,7Z,ARJ,BZ,CPIO_CRC,CPIO_NEWC,CPIO_ODC,,JAR,LHA,MSCAB,MSSZDD,OLD_TAR,POSIX_TAR,RAR,SIS,SIT,ZIP,ZIP_ENC,ACCDB,HLP,MAIL,MDB, MDI,MNY,MSCHM,MSOLE2,MSWORD_MAC5,MWL,NEW_OFFICE,ONE,PST,RTF,TNEF,WAB,WP,WRI,XLW,XPS. Adicionalmente, deve implementar em tempo real a inspeção, detecção e bloqueio autônomo (prevenção sem a necessidade de integrar com outros sistemas terceiros para que seja feito o bloqueio da ameaça) na rede para os seguintes tipos de arquivos: 7Z, ACCDB, ARJ, BINARY_DATA, BINHEX, BZ, CPIO_CRC, CPIO_NEWC, CPIO, ODC, EICAR, FLV, GZ, ISHIELD_MSI, JAR, JARPACK, LHA, MAIL, MDB, MDI, MNY, MSCAB, MSCHM, MSEXE, MSOLE2, MSWORD_MAC5, NEW_OFFICE, OLD_TAR, PDF, POSIX_TAR, PST, RAR, RTF, SIS, SIT, SWF, TNEF, WAB, WRI, XLW, XPS, ZIP, ZIP_ENC;

8.5.5.23. Deve implementar atualização a base de dados da Rede de Inteligência de forma automático, permitindo o agendamento mínimo de 2 hora de intervalo;

8.5.5.24. Para recursos de análise virtualizada existente, deve ser mantido um histórico dos resultados de avaliações prévias de um arquivo e utilizar esta informação para determinar de forma configurável que o arquivo seja considerado malware a partir de certo limite;

8.5.5.25. Dispor de múltiplos motores e mecanismos de detecção e prevenção para verificação de Malwares e códigos maliciosos incluindo:

8.5.5.25.1. Machine learning;

8.5.5.25.2. Fuzzy fingerprinting;

8.5.5.25.3. Reputação global;

8.5.5.25.4. Detecção customizada local por blacklist e regras customizadas de detecção de tráfego de rede;

8.5.5.25.5. Análise dinâmica (sandbox).

8.5.5.26. O processo de análise de comunicações, Malwares e sua prevenção deve ocorrer em tempo real, não sendo aceitas tecnologias que dependam de verificações que induzam latência suficiente para postergar a entrega de arquivos ao seu destino original;

8.5.5.27. Deve permitir exportar o resultado das análises de malwares de dia Zero em PDF e CSV a partir da própria interface de gerência;

8.5.5.28. Deve permitir o download dos malwares identificados a partir da própria interface de gerência;

8.5.5.29. Deve permitir visualizar os resultados das análises de malwares de dia zero nos diferentes sistemas operacionais suportados;

8.5.5.30. Deve permitir informar ao fabricante quanto a suspeita de ocorrências de falso-positivo e falso-negativo na análise de malwares de Dia Zero a partir da própria interface de gerência;

8.5.5.31. Caso a solução seja fornecida em appliance local, deve possuir, no mínimo, 8 ambientes controlados (sand-box) independentes para execução simultânea de arquivos suspeitos;

8.5.5.32. Caso sejam necessárias licenças de sistemas operacional e softwares para execução de arquivos no ambiente controlado (sand-box), as mesmas devem ser fornecidas em sua totalidade, sem custos adicionais para a contratante;

8.5.5.33. Suportar a análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL no ambiente controlado;

8.5.5.34. Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos java (.jar e .class).

8.5.6. Permitir o envio de arquivos para análise no ambiente controlado de forma automática via API;

8.5.7. **FILTRO DE URL:**

8.5.7.1. Deve possuir as seguintes funcionalidades de filtro de URL;

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

8.5.7.3. 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;

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

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

8.5.7.6. Possuir pelo menos 80 categorias de URLs pré-definidas/default;

8.5.7.7. Possuir o mínimo de 280 milhões de URLs categorizadas;

8.5.7.8. Permitir a criação de categorias de URLs customizadas;

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

8.5.7.10. Permitir a customização de página de bloqueio;

8.5.7.11. 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).

8.5.8. **IDENTIFICAÇÃO DE USUÁRIOS:**

8.5.8.1. 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;

8.5.8.2. 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;

8.5.8.3. 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;

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

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

8.5.8.6. 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);

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

8.5.9. **FILTRO DE DADOS:**

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

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

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

8.5.9.4. Suportar identificação de arquivos compactados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

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

8.5.9.6. 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.

8.5.10. **GEO-LOCALIZAÇÃO:**

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

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

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

8.5.11. **VPN:**

8.5.11.1. Suportar VPN Site-to-Site;

8.5.11.2. Suportar IPSec VPN;

8.5.11.3. A VPN IPSEc deve suportar:

8.5.11.3.1. 3DES;

8.5.11.3.2. Autenticação MD5 e SHA-1;

8.5.11.3.3. Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;

8.5.11.3.4. Algoritmo Internet Key Exchange (IKEv1 e v2);

8.5.11.3.5. AES 128, 192 e 256 (Advanced Encryption Standard);

8.5.11.3.6. Autenticação via certificado IKE PKI.

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

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

8.5.11.6. Suportar autenticação via AD/LDAP, certificado e base de usuários local;

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

8.6. **SOLUÇÃO DE GERÊNCIA E RELATÓRIOS do FIREWALL NGFW:**

8.6.1. A solução ofertada deverá ser entregue como appliance virtual para instalação no datacenter virtualizado da Prefeitura Municipal de Foz do Iguaçu (VMWare ESXi). Além disso também deverão ser entregues o software, licenças, assim como quaisquer outros componentes necessários a seu pleno funcionamento;

8.6.2. A solução ofertada não pode ser baseada em Código aberto ou Software livre;

8.6.3. Não serão aceitas licenças tipo DEMO;

8.6.4. Deve suportar instalação nas seguintes plataformas:VMWare, KVM e cloud AWS.

8.6.5. A solução ofertada deve ser desenvolvida e comercializada pelo mesmo fabricante do Firewall NGFW ofertado no item anterior;

8.6.6. A solução deve suportar no mínimo 25 appliances firewall NGFW;

8.6.7. A solução deve estar licenciada para 2 appliances firewall NGFW;

8.6.8. As funcionalidades de gerência e retenção de logs que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação;

8.6.9. Centralizar os logs e relatórios do cluster, usando uma única interface de gerenciamento;

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

8.6.11. A solução gerencia deve permitir nativamente conexão com nuvem de cybersegurança de terceiros através da linguagem padrão STIX TAXII;

8.6.12. O armazenamento poderá ser realizado através de composição com solução de terceiros como por exemplo SIEM (*Security Information Management*);

8.6.13. Não será permitido a instalação de cliente para administração do appliance de Firewall;

8.6.14. O gerenciamento deve permitir/possuir:

8.6.14.1. Visualização de logs e relatórios relacionados às políticas de firewall e controle de aplicação;

8.6.14.2. Visualização de logs e relatórios relacionados às IPS, Controle de Aplicação e Anti-Malware;

8.6.14.3. Visualização de logs e relatórios relacionados às políticas de Filtro de URL;

8.6.14.4. Monitoração de logs;

8.6.14.5. Ferramentas de investigação de logs;

8.6.14.6. Visualização das capturas de pacotes realizadas nos ataques detectados;

8.6.14.7. Acesso concorrente de administradores.

8.6.15. Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

8.6.16. Deve permitir monitorar eventos diretamente relacionados a identificação de aplicação e análise de ameaças como, mas não limitado à ocorrência de botnets, ocorrência de vírus na rede e acesso a sites de grupos extremistas ou pedofilia;

8.6.17. Bloqueio de alterações, no caso acesso simultâneo de dois ou mais administradores;

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

8.6.19. Autenticação integrada ao Microsoft Active Directory (AD) e servidor Radius;

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

8.6.21. Deverá ter a capacidade de gerar um relatório gráfico que permita visualizar as mudanças na utilização de aplicações na rede no que se refere a um período de tempo anterior, permitindo comparar os diferentes consumos realizados pelas aplicações no decorrer do tempo;

8.6.22. Deve prover relatórios com visão correlacionada de aplicações, ameaças (IPS, Antivírus e Anti-Spware), URLs e filtro de arquivos, para melhor diagnóstico e resposta a incidentes;

8.6.23. Deve permitir a criação de painéis de instrumentos (dashboards) ou relatórios customizados para visibilidades do tráfego de aplicativos, usuários, categorias de URL, ameaças identificadas pelo IPS, ameaças identificadas pelo malwares detectados, apliacações mais utilizadas, protocolos mais utilizados, principais atacantes (com informação de geolocalização);

8.6.24. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos dispositivos de segurança;

8.6.25. Deve prover uma visualização sumarizada das aplicações e URLs que passaram pela solução;

8.6.26. Deve possuir mecanismo "Drill-Down" para navegação nos dashboards em tempo real;

8.6.27. Deve ser possível exportar os logs em CSV;

8.6.28. Deve permitir que os logs e relatórios sejam rotacionados automaticamente baseado no tempo em que estão armazenados na solução;

8.6.29. Exibição das seguintes informações, de forma histórica ou em tempo real:

8.6.29.1. Situação do dispositivo e do cluster;

8.6.29.2. Principais aplicações;

8.6.29.3. Principais aplicações por risco;

8.6.29.4. Principais ameaças;

8.6.29.5. Uso de CPU e memória.

8.6.30. No mínimo os seguintes relatórios devem ser gerados:

8.6.30.1. Resumo gráfico de aplicações utilizadas;

8.6.30.2. Principais hosts por número de ameaças identificadas;

8.6.30.3. Atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL, ameaças de rede vinculadas a este tráfego;

8.6.30.4. Deve permitir a criação de relatórios personalizados.

8.6.31. Gerar alertas automáticos via:

8.6.31.1. Email;

8.6.31.2. SNMP;

8.6.31.3. Syslog.

8.6.32. O gerenciamento deve permitir/possuir:

8.6.32.1. Criação e administração de políticas de firewall e controle de aplicação;

8.6.32.2. Criação e administração de políticas de IPS e Anti-Malware;

8.6.32.3. Criação e administração de políticas de Filtro de URL;

8.6.32.4. Deve permitir usar palavras chaves e cores para facilitar identificação de regras;

8.6.32.5. Alerta de alterações, no caso acesso simultâneo de dois ou mais administradores;

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

8.6.32.7. Autenticação integrada ao Microsoft Active Directory (AD) e servidor Radius;

8.6.32.8. Localização de em quais regras um endereço IP, IP Range, subnet ou objetos estão sendo utilizados;

8.6.32.9. Backup das configurações e rollback de configuração para a última configuração salva;

8.6.32.10. Deve possuir mecanismo de validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras;

8.6.32.11. Deve possibilitar a visualização e comparação de configurações atuais, configuração anterior e configurações antigas.

8.7. ***Switch* Tipo I (agregador layer 2):**

8.7.1. Switch de acesso com 16 portas 10/100/1000 Mbps UTP e 2 slots SFP 1000 Mbps;

8.7.2. Deve suportar alimentação elétrica redundante capaz de suportar o equipamento com todas as funcionalidades;

8.7.3. Deve permitir ser empilhado com todos os switches empilháveis constantes neste grupo, formando uma entidade lógica única e permitindo usar agregação de links entre switches diferentes da mesma pilha;

8.7.4. Deve implementar, no mínimo, 1023 vlans simultaneamente;

8.7.5. Deve possuir switching bandwidth full-duplex de, no mínimo, 30 Gbps e taxa de encaminhamento de, no mínimo, 25.5 Mpps;

8.7.6. Deve possuir, no mínimo, 18 portas ativas sendo 16 portas Ethernet 10/100/1000 autosensing com conectores RJ-45 e 2 slots 1000 Mbps do tipo SFP (módulos/transceiver) não inclusos, full-duplex, para fibras óticas ou UTP;

8.7.7. As interfaces 10/100/1000 devem obedecer às normas técnicas IEEE802.3 (10BaseT), IEEE802.3u (100BaseTX), 802.3ab (1000BaseT) e IEEE802.3x (Flow Control);

8.7.8. Deve implementar DHCP Relay em múltiplas VLANS;

8.7.9. Deve permitir a criação de listas de acesso baseadas em endereço IP para limitar o acesso ao switch via Telnet, SSH e SNMP. Deve ser possível definir os endereços IP de origem das sessões Telnet e SSH;

8.7.10. Deve implementar listas de controle de acesso (ACLs) baseadas em endereço IP de origem e destino, portas TCP e UDP de origem e destino;

8.7.11. Deve possuir análise do protocolo ARP (Address Resolution Protocol) e possuir proteção nativa contra-ataques do tipo "ARP Poisoning";

8.7.12. Deve ser possível definir, por porta, o intervalo de tempo para obrigar o cliente a se reautenticar (reautenticação periódica);

8.7.13. Deve ser possível forçar manualmente a reautenticação de um usuário conectado a uma porta do switch habilitada para 802.1x;

8.7.14. Deve ter tratamento de autenticação 802.1x diferenciado entre "Voice Vlan" e "Data LAN", na mesma porta para que um erro de autenticação em uma Vlan não interfira na outra;

8.7.15. Deve implementar padrão IEEE 802.3at;

8.7.16. Deve implementar padrão IEEE 802.3af;

8.7.17. Deve suportar QoS Traffic Policing;

8.7.18. Deve também oferecer suporte aos mecanismos de QoS WRR (Weighted Round Robin) e WRED (Weighted Random Early Detection);

8.7.19. Deve permitir Classificação e Reclassificação baseadas em endereço IP de origem/destino, portas TCP e UDP de origem e destino, endereços MAC de origem e destino;

8.7.20. Deve permitir Classificação, Marcação e Remarcação baseadas em CoS ("Class of Service" - nível 2) e DSCP ("Differentiated Services Code Point"- nível 3), conforme definições do IETF (Internet Engineering Task Force);

8.7.21. Deve ser possível a especificação de banda por classe de serviço;

8.7.22. Para os pacotes que excederem a especificação, deve ser possível configurar ações tais como: transmissão do pacote sem modificação, transmissão com remarcação do valor de DSCP, descarte do pacote;

8.7.23. Montável em rack 19" incluindo todos os acessórios necessários;

8.7.24. Deve possuir fonte de alimentação AC bivolt, com seleção automática de tensão (na faixa de 100 a 240V) e de frequência (de 50/60 Hz);

8.7.25. Deve possuir cabo de alimentação para a fonte com, no mínimo, 1,00m (um metro) de comprimento com plugue no padrão brasileiro (NBR 14136:2002);

8.7.26. Deve possibilitar a configuração dinâmica de portas por software, permitindo a definição de portas ativas/inativas;

8.7.27. Deve possuir porta de console para ligação direta e através de terminal RS-232 para acesso à interface de linha de comando. Poderá ser fornecida porta de console com interface USB;

8.7.28. Deve possuir LEDs para a indicação do status das portas e atividade, além de duplex. Os switchs PoE deverão possuir LEDs que indiquem a utilização desta solução;

8.7.29. Todas as portas UTP devem suportar configuração Half-Duplex e Full-Duplex, com a opção de negociação automática;

8.7.30. Todas as portas UTP devem suportar autoconfiguração de crossover (Auto MDIX);

8.7.31. Deve possuir capacidade de associação das portas 10/100, 10/100/1000 ou das portas 1G, no mínimo, em grupo de até oito portas, formando uma única interface lógica com as mesmas facilidades das interfaces originais. Dever ser compatível com a norma IEEE 802.3ad e permitir a formação de, no mínimo, 6 grupos de portas;

8.7.32. Deve possuir capacidade para, pelo menos, 8.000 endereços MAC na tabela de comutação;

8.7.33. Deve suportar Jumbo Frames de, no mínimo, 9016 Bytes;

8.7.34. Deve implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps;

8.7.35. Deve implementar, pelo menos, os níveis AuthNoPriv, authNoPriv e authPriv de segurança para SNMPv3;

8.7.36. Possuir criptografia 3DES e AES para proteção dos dados de gerência SNMPv3;

8.7.37. Deve possuir suporte a MIB II, conforme RFC 1213;

8.7.38. Deve implementar a MIB privativa que forneça informações relativas ao funcionamento do equipamento;

8.7.39. Deve possuir descrição completa da MIB implementada no equipamento, inclusive a extensão privativa;

8.7.40. Deve possibilitar a obtenção da configuração do equipamento através do protocolo SNMP;

8.7.41. Deve possuir armazenamento interno das mensagens de log geradas pelo equipamento de, no mínimo, 2048 bytes;

8.7.42. Deve possibilitar a obtenção via SNMP de informações de capacidade e desempenho da CPU, memória e portas;

8.7.43. Deve permitir o controle da geração de traps por porta, possibilitando restringir a geração de traps para portas específicas;

8.7.44. Deve implementar nativamente 4 grupos RMON (History, Statistcs, Alarms e Events) conforme a RFC 1757;

8.7.45. Deve implementar o protocolo LLDP (IEEE 802.1AB);

8.7.46. Deve implementar Telnet para acesso à interface de linha de comando;

8.7.47. Deve permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interfaces ethernet e serial;

8.7.48. Deve ser configurável e gerenciável via GUI (graphical user interface), CLI (command line interface), SNMP, Telnet, SSH, FTP, HTTP e HTTPS com, no mínimo, 5 sessões simultâneas e independentes;

8.7.49. Deve permitir a atualização de sistema operacional através do protocolo TFTP ou FTP;

8.7.50. Deve permitir a transferência segura de arquivos para o equipamento através do protocolo SCP (Secure Copy) utilizando um cliente padrão ou SFTP (Secure FTP);

8.7.51. Deve suportar protocolo SSH para gerenciamento remoto, implementando pelo menos o algoritmo de encriptação de dados 3DES;

8.7.52. Deve permitir que a sua configuração seja feita através de terminal assíncrono;

8.7.53. Deve permitir tanto a gravação de log em equipamento externo (syslog) como visualização interna (no próprio equipamento);

8.7.54. Deve permitir o armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior à queda de alimentação;

8.7.55. Deve possuir ferramentas para depuração e gerenciamento em primeiro nível, tais como debug, trace e log de eventos;

8.7.56. Deve implementar VLANs por porta no padrão IEEE 802.1q;

8.7.57. Deve implementar mecanismo de seleção de quais VLANs serão permitidas no trunk 802.1q, de forma dinâmica;

8.7.58. Deve permitir o espelhamento da totalidade do tráfego de uma porta, de um grupo de portas e de VLANs para outra porta localizada no mesmo switch;

8.7.59. Deve ser possível definir o sentido do tráfego a ser espelhado (somente tráfego de entrada, somente tráfego de saída ou ambos simultaneamente);

8.7.60. Deve implementar funcionalidade de separação do tráfego de voz e dados em uma mesma porta de acesso (Voice VLAN);

8.7.61. Deve ser possível estabelecer quais VLANs serão permitidas em cada um dos trunks configurados;

8.7.62. Deve permitir a criação, remoção, gerenciamento e distribuição de VLANs de forma dinâmica através de portas configuradas como tronco IEEE 802.1Q;

8.7.63. Deve implementar o protocolo NTPv4 (Network Time Protocol, versão 4). Deve ser suportada autenticação e criptografia entre os peers NTP, conforme definições da RFC 5905;

8.7.64. Deve implementar DHCP Server em múltiplas VLANS;

8.7.65. Deve implementar DHCP Option 82;

8.7.66. Deve implementar mecanismo de autenticação para acesso local ou remoto ao equipamento baseada em um Servidor de Autenticação/Autorização do tipo TACACS e RADIUS;

8.7.67. Deve proteger a interface de comando do equipamento através de senha;

8.7.68. Deve implementar o protocolo SSH V2 para acesso à interface de linha de comando;

8.7.69. Deve possibilitar o estabelecimento do número máximo de MACs que podem estar associados a uma dada porta do switch. Deve ser possível desabilitar a porta e enviar traps SNMP caso o número de endereços MAC configurados para a porta seja excedido;

8.7.70. Deve permitir a associação de um endereço MAC específico a uma dada porta do switch, de modo que somente a estação que tenha tal endereço possa usar a referida porta para conexão;

8.7.71. Deve implementar mecanismos de AAA (Authentication, Authorization e Accounting) com garantia de entrega;

8.7.72. Deve possuir controle de broadcast, multicast e unicast por porta;

8.7.73. Deve implementar a criptografia de todos os pacotes enviados ao servidor de controle de acesso e não só os pacotes referentes à senha;

8.7.74. Deve permitir o controle de privilégios em comandos e acesso aos elementos de rede, definidos para usuários e grupos de usuários;

8.7.75. Deve possuir suporte a mecanismo de proteção da "Root Bridge" do algoritmo "Spanning-Tree" para defesa contra-ataques do tipo "Denial of Service" no ambiente nível 2;

8.7.76. Deve possuir suporte à suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta do switch esteja colocada no modo "Fast Forwarding" (conforme previsto no padrão IEEE 802.1w);

8.7.77. Deve possuir análise do protocolo DHCP e permitir que se crie uma tabela de associação entre endereços IP atribuídos dinamicamente, MAC da máquina que recebeu o endereço e porta física do switch em que se localiza tal MAC;

8.7.78. Deve possuir método de segurança que utilize uma tabela criada pelo mecanismo de análise do protocolo DHCP, permitindo a filtragem de tráfego IP que possua uma origem diferente do endereço IP atribuído pelo Servidor de DHCP. Essa filtragem deve ser por porta;

8.7.79. Deve implementar padrão IEEE 802.1d (Spanning Tree Protocol);

8.7.80. Deve implementar padrão IEEE 802.1q (Vlan Frame Tagging);

8.7.81. Deve implementar padrão IEEE 802.1p (Class of Service) para cada porta;

8.7.82. Deve implementar padrão IEEE 802.3ad (Link Aggregation Control Protocol - LACP);

8.7.83. Deve implementar padrão IEEE 802.1w (Rapid spanning Tree Protocol);

8.7.84. Deve implementar padrão IEEE 802.1s (Multi-Instance Spanning-Tree), com suporte a, no mínimo, 64 instâncias simultâneas do protocolo Spanning-Tree;

8.7.85. Deve implementar PVST ou PVST+;

8.7.86. Os processos de Autenticação, Autorização e Accounting associados a controle de acesso administrativo ao equipamento devem ser completamente independentes dos processos AAA no contexto 802.1x;

8.7.87. Deve implementar controle de acesso por porta, usando o padrão IEEE 802.1x (Port Based Network Access Control). Deve atender, no mínimo, a funcionalidades de designação de VLAN específica para o usuário, caso a estação não possua cliente 802.1x (suplicante) ou as credenciais do usuário não estejam corretas (falha de autenticação);

8.7.88. Deve implementar associação automática de VLAN da porta do switch através da qual o usuário requisitou acesso à rede (802.1x VLAN Assignment);

8.7.89. Deve implementar "accounting" das conexões IEEE 802.1x. O switch (cliente AAA) deve ser capaz de enviar, ao servidor AAA, pelo menos as seguintes informações sobre a conexão: nome do usuário, switch em que o computador do usuário está conectado, porta do switch utilizada por acesso, endereço MAC da máquina utilizada pelo usuário, endereço IP do usuário, horários de início e término da conexão e bytes transmitidos e recebidos durante a conexão;

8.7.90. Deve suportar a autenticação 802.1x via endereço MAC em substituição à identificação de usuário, para equipamentos que não disponham de suplicantes;

8.7.91. Deve suportar a autenticação 802.1x através dos protocolos EAP-MD5, PEAP e EAP-TLS;

8.7.92. Deve implementar suporte ao serviço DHCP Server em múltiplas VLANS simultaneamente, para que possa atribuir endereços IP aos clientes 802.1x autenticados e autorizados;

8.7.93. Deve ser suportada a autenticação de múltiplos usuários em uma mesma porta;

8.7.94. Deve implementar filtragem de pacotes (ACL - Access Control List);

8.7.95. Deve possuir a facilidade de priorização de tráfego através do protocolo IEEE 802.1p;

8.7.96. Deve possuir suporte a uma fila com prioridade estrita (prioridade absoluta em relação às demais classes dentro do limite de banda que lhe foi atribuído) para tratamento do tráfego "real-time" (voz e vídeo);

8.7.97. Deve suportar funcionalidades de QoS Traffic Shaping;

8.7.98. Deve oferecer suporte ao mecanismo de QoS SRR (Shaped Round Robin);

8.7.99. Deve implementar pelo menos quatro filas de prioridade por porta de saída (egress port);

8.7.100. Deve implementar em todas as interfaces do switch o protocolo IGMP Snooping (v1, v2 e v3), não permitindo que o tráfego MULTICAST seja tratado como broadcast no switch;

8.7.101. Deve implementar em todas as interfaces do switch o protocolo MLD Snooping (v1 e v2), não permitindo que o tráfego MULTICAST IPv6 seja tratado como broadcast no switch;

8.7.102. O switch deve ter a capacidade de identificar, ao menos, pelos seguintes mecanismos MAC, OUI, LLDP, MAB e 8021.X os equipamentos diretamente conectados à qualquer uma das interfaces do dispositivo. Ao identificar este equipamento deve ser capaz de configurar automaticamente a interface a que este equipamento estiver conectado, aplicando desde descrição da porta até as políticas de segurança e qualidade de serviço da mesma;

8.7.103. O switch deve ser capaz de implementar funcionalidades para visualização de consumo, desabilitando interfaces em horários pré-determinados que estejam alimentando equipamentos;

8.7.104. Deve suportar UniDirectional Link Detection Protocol (UDLD) e Aggressive UDLD para detectar problemas de conexão ou problemas em um cabo de fibra óptica, desativando as portas do switch;

8.7.105. Deve implementar TDR (Time Domain Reflectometer) para detectar, caracterizar e localizar falhas nos cabos metálicos tanto nas interfaces UTP como nas interfaces de duplo propósito.

8.8. ***Switch Tipo* 2 (*core*):**

8.8.1. Switch Layer 3 com 48 portas Gigabit Ethernet do tipo SFP com suporte a 10Gigabit Ethernet;

8.8.2. Deve implementar, no mínimo, 1000 vlans simultaneamente;

8.8.3. Deve possuir switching bandwidth full-duplex de, no mínimo, 176 Gbps e taxa de encaminhamento de, no mínimo, 130 Mpps;

8.8.4. Deve possuir, no mínimo, 48 portas ativas sendo 48 slots SFP Gigabit Ethernet com transceivers inclusos, full-duplex, para UTP;

8.8.5. Os transceivers devem obedecer às normas técnicas IEEE802.3 (10BaseT), IEEE802.3u (100BaseTX), 802.3ab (1000BaseT) e IEEE802.3x (Flow Control);

8.8.6. Com a finalidade de Uplink, deve conter ou suportar a instalação de até 2(duas) portas de 10Gigabit Ethernet do tipo SFP+, com transceivers do tipo 10GBASE-SR, LR, LRM, CX1. O suporte poderá ser feito através da instalação de módulo de expansão;

8.8.7. Com a finalidade de Uplink, deve conter ou suportar a instalação de até 2 (duas) portas Gigabit Ethernet do tipo SFP. Não será aceito porta (s) compartilhada (s) (COMBO) com os 48 slots SFP Gigabit. O suporte poderá ser feito através da instalação de módulo de expansão;

8.8.8. Deve suportar empilhamento físico com cabos de empilhamento dedicados, não podendo ser utilizados portas 10Gbps com SFP+ para empilhamento, permitindo empilhamento de até 9 unidades iguais, com velocidade de empilhamento de pelo menos 400 Gbps (full-duplex). O empilhamento deve acontecer em anel, não podendo utilizar nenhuma das portas acima descritas. Deve ser fornecido com o cabo para tal recurso;

8.8.9. Quando empilhados, a pilha deve suportar ser gerenciada através de um único endereço IP, permitir agregação lógica de links utilizando qualquer porta da pilha e permitir espelhamento de portas de qualquer porta para qualquer porta da pilha;

8.8.10. Ao adicionar ou remover switches do empilhamento a inserção e remoção deve ser transparente e automática, sem necessidade de configurações manuais e sem necessidade de se reinicializar a pilha;

8.8.11. Deve implementar tecnologia de empilhamento que permita a propagação de configurações de QoS através da pilha sem necessidade de intervenção manual;

8.8.12. Montável em rack 19" incluindo todos os acessórios necessários;

8.8.13. Deve possuir fonte de alimentação AC bivolt, com seleção automática de tensão (na faixa de 100 a 240V) e de frequência (de 50/60 Hz), com possibilidade de instalação de fonte redundante;

8.8.14. Deve suportar fonte de alimentação redundante interna ao chassi de, no mínimo, 350W. O switch deve suportar até quatro switches empilhados através de porta específica para compartilhamento dos recursos de alimentação (Fonte de alimentação) garantindo total redundância da pilha;

8.8.15. Deve possuir cabo de alimentação para a fonte com, no mínimo, 1,00m (um metro) de comprimento com plugue no padrão brasileiro (NBR 14136:2002);

8.8.16. Deve possibilitar a configuração dinâmica de portas por software, permitindo a definição de portas ativas/inativas;

8.8.17. Deve possuir porta de console para ligação direta e através de terminal RS-232 para acesso à interface de linha de comando. Poderá ser fornecida porta de console com interface USB;

8.8.18. Deve possuir LEDs para a indicação do status das portas e atividade;

8.8.19. Deve possuir capacidade para, pelo menos, 12.000 endereços MAC na tabela de comutação;

8.8.20. Deve suportar Jumbo Frames de, no mínimo, 9016 Bytes;

8.8.21. O sistema operacional do equipamento deve ser armazenado em memória tipo Flash, com capacidade adequada para acomodá-lo em sua configuração máxima;

8.8.22. Deve implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps;

8.8.23. Deve implementar, pelo menos, os níveis AuthNoPriv, authNoPriv e authPriv de segurança para SNMPv3;

8.8.24. Possuir criptografia 3DES e AES para proteção dos dados de gerência SNMPv3.

8.8.25. Deve possuir suporte a MIB II, conforme RFC 1213;

8.8.26. Deve implementar a MIB privativa que forneça informações relativas ao funcionamento do equipamento;

8.8.27. Deve possuir descrição completa da MIB implementada no equipamento, inclusive a extensão privativa;

8.8.28. Deve possibilitar a obtenção da configuração do equipamento através do protocolo SNMP;

8.8.29. Deve possuir armazenamento interno das mensagens de log geradas pelo equipamento de, no mínimo, 2048 bytes;

8.8.30. Deve possibilitar a obtenção via SNMP de informações de capacidade e desempenho da CPU, memória e portas;

8.8.31. Deve permitir o controle da geração de traps por porta, possibilitando restringir a geração de traps para portas específicas;

8.8.32. Deve implementar nativamente 4 grupos RMON (History, Statistcs, Alarms e Events) conforme a RFC 1757;

8.8.33. Deve implementar o protocolo LLDP (IEEE 802.1AB);

8.8.34. Deve implementar Telnet para acesso à interface de linha de comando;

8.8.35. Deve permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interfaces ethernet e serial;

8.8.36. Deve ser configurável e gerenciável via GUI (graphical user interface), CLI (command line interface), SNMP, Telnet, SSH, FTP, HTTP e HTTPS com, no mínimo, 5 sessões simultâneas e independentes;

8.8.37. Deve permitir a atualização de sistema operacional através do protocolo TFTP ou FTP;

8.8.38. Deve permitir a transferência segura de arquivos para o equipamento através do protocolo SCP (Secure Copy) utilizando um cliente padrão ou SFTP (Secure FTP);

8.8.39. Deve suportar protocolo SSH para gerenciamento remoto, implementando pelo menos o algoritmo de encriptação de dados 3DES;

8.8.40. Deve permitir que a sua configuração seja feita através de terminal assíncrono;

8.8.41. Deve permitir tanto a gravação de log em equipamento externo (syslog) como visualização interna (no próprio equipamento);

8.8.42. Deve permitir o armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior à queda de alimentação;

8.8.43. Deve possuir ferramentas para depuração e gerenciamento em primeiro nível, tais como debug, trace e log de eventos;

8.8.44. Deve implementar VLANs por porta no padrão IEEE 802.1q;

8.8.45. Deve implementar mecanismo de seleção de quais VLANs serão permitidas no trunk 802.1q, de forma dinâmica;

8.8.46. Deve permitir o espelhamento da totalidade do tráfego de uma porta, de um grupo de portas e de VLANs para outra porta localizada no mesmo switch;

8.8.47. Deve ser possível definir o sentido do tráfego a ser espelhado (somente tráfego de entrada, somente tráfego de saída ou ambos simultaneamente);

8.8.48. Deve implementar funcionalidade de separação do tráfego de voz e dados em uma mesma porta de acesso (Voice VLAN), independente de fabricante;

8.8.49. Deve permitir a criação de subgrupos dentro de uma mesma VLAN com conceito de portas isoladas e portas compartilhadas (“promíscuas”), onde portas isoladas não se comunicam com outras portas isoladas, mas apenas com as portas compartilhadas (“promíscuas”) de uma dada VLAN;

8.8.50. Deve ser possível estabelecer quais VLANs serão permitidas em cada um dos trunks configurados;

8.8.51. Deve permitir a criação, remoção, gerenciamento e distribuição de VLANs de forma dinâmica através de portas configuradas como tronco IEEE 802.1Q;

8.8.52. Deve implementar o protocolo NTPv4 (Network Time Protocol, versão 4). Deve ser suportada autenticação e criptografia entre os peers NTP, conforme definições da RFC 5905;

8.8.53. Deve implementar DHCP Server em múltiplas VLANS;

8.8.54. Deve implementar DHCP Option 82;

8.8.55. Deve implementar roteamento estático de, no mínimo, 16 rotas;

8.8.56. Deve ser fornecido com recursos instalados para roteamento RIP versão 1 (RFC1058), RIP versão 2 (RFC2453) e RIPng;

8.8.57. Deve suportar roteamento OSPF com, no mínimo, 1 instância e 200 rotas;

8.8.58. Deve implementar Virtual routing and forwarding (VRF)-Lite;

8.8.59. Deve suportar roteamento multicast através dos protocolos PIM Sparse Mode e DVMRP Distance Vector Multicast Routing Protocol;

8.8.60. Deve ser fornecido com recursos instalados para a implementação do protocolo VRRP ou similar;

8.8.61. Deve implementar mecanismo de autenticação para acesso local ou remoto ao equipamento baseada em um Servidor de Autenticação/Autorização do tipo TACACS e RADIUS;

8.8.62. Deve proteger a interface de comando do equipamento através de senha;

8.8.63. Deve implementar o protocolo SSH V2 para acesso à interface de linha de comando;

8.8.64. Deve possibilitar o estabelecimento do número máximo de MACs que podem estar associados a uma dada porta do switch. Deve ser possível desabilitar a porta e enviar traps SNMP caso o número de endereços MAC configurados para a porta seja excedido;

8.8.65. Deve permitir a associação de um endereço MAC específico a uma dada porta do switch, de modo que somente a estação que tenha tal endereço possa usar a referida porta para conexão;

8.8.66. Deve implementar mecanismos de AAA (Authentication, Authorization e Accounting) com garantia de entrega;

8.8.67. Deve possuir controle de broadcast, multicast e unicast por porta através de comandos específicos;

8.8.68. Deve implementar a criptografia de todos os pacotes enviados ao servidor de controle de acesso e não só os pacotes referentes à senha;

8.8.69. Deve permitir o controle de privilégios em comandos e acesso aos elementos de rede, definidos para usuários e grupos de usuários;

8.8.70. Deve possuir suporte a mecanismo de proteção da "Root Bridge" do algoritmo "Spanning-Tree" para defesa contra ataques do tipo "Denial of Service" no ambiente nível 2;

8.8.71. Deve possuir suporte à suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta do switch esteja colocada no modo "Fast Forwarding" (conforme previsto no padrão IEEE 802.1w);

8.8.72. Deve possuir análise do protocolo DHCP e permitir que se crie uma tabela de associação entre endereços IP atribuídos dinamicamente, MAC da máquina que recebeu o endereço e porta física do switch em que se localiza tal MAC;

8.8.73. Deve possuir método de segurança que utilize uma tabela criada pelo mecanismo de análise do protocolo DHCP, permitindo a filtragem de tráfego IP que possua uma origem diferente do endereço IP atribuído pelo Servidor de DHCP. Essa filtragem deve ser por porta;

8.8.74. Deve implementar padrão IEEE 802.1d (Spanning Tree Protocol);

8.8.75. Deve implementar padrão IEEE 802.1q (Vlan Frame Tagging);

8.8.76. Deve implementar padrão IEEE 802.1p (Class of Service) para cada porta;

8.8.77. Deve implementar padrão IEEE 802.3ad (Link Aggregation Control Protocol - LACP);

8.8.78. Deve implementar padrão IEEE 802.1w (Rapid spanning Tree Protocol);

8.8.79. Deve implementar padrão IEEE 802.1s (Multi-Instance Spanning-Tree), com suporte a, no mínimo, 64 instâncias simultâneas do protocolo Spanning-Tree;

8.8.80. Deve implementar PVST ou PVST+;

8.8.81. Os processos de Autenticação, Autorização e Accounting associados a controle de acesso administrativo ao equipamento devem ser completamente independentes dos processos AAA no contexto 802.1x;

8.8.82. Deve implementar controle de acesso por porta, usando o padrão IEEE 802.1x (Port Based Network Access Control). Deve atender, no mínimo, a funcionalidades de designação de VLAN específica para o usuário, caso a estação não possua cliente 802.1x (suplicante) ou as credenciais do usuário não estejam corretas (falha de autenticação);

8.8.83. Deve implementar associação automática de VLAN da porta do switch através da qual o usuário requisitou acesso à rede (802.1x VLAN Assignment);

8.8.84. Deve implementar "accounting" das conexões IEEE 802.1x. O switch (cliente AAA) deve ser capaz de enviar, ao servidor AAA, pelo menos as seguintes informações sobre a conexão: nome do usuário, switch em que o computador do usuário está conectado, porta do switch utilizada por acesso, endereço MAC da máquina utilizada pelo usuário, endereço IP do usuário, horários de início e término da conexão e bytes transmitidos e recebidos durante a conexão;

8.8.85. Deve suportar a autenticação 802.1x via endereço MAC em substituição à identificação de usuário, para equipamentos que não disponham de suplicantes;

8.8.86. Deve suportar a autenticação 802.1x através dos protocolos EAP-MD5, PEAP e EAP-TLS;

8.8.87. Deve implementar suporte ao serviço DHCP Server em múltiplas VLANS simultaneamente, para que possa atribuir endereços IP aos clientes 802.1x autenticados e autorizados;

8.8.88. Deve ser suportada a autenticação de múltiplos usuários em uma mesma porta;

8.8.89. Deve implementar filtragem de pacotes (ACL - Access Control List);

8.8.90. Deve possuir a facilidade de priorização de tráfego através do protocolo IEEE 802.1p;

8.8.91. Deve possuir suporte a uma fila com prioridade estrita (prioridade absoluta em relação às demais classes dentro do limite de banda que lhe foi atribuído) para tratamento do tráfego "real-time" (voz e vídeo);

8.8.92. Deve suportar funcionalidades de QoS Traffic Shaping;

8.8.93. Deve oferecer suporte ao mecanismo de QoS SRR (Shaped Round Robin) ou Weighted Round Robin (WRR);

8.8.94. Deve implementar pelo menos 4 (quatro) filas de prioridade por porta de saída (egress port);

8.8.95. Deve implementar pelo menos 2 (duas) filas de prioridade de entrada;

8.8.96. Deve implementar em todas as interfaces do switch o protocolo IGMP Snooping (v1, v2 e v3), não permitindo que o tráfego MULTICAST seja tratado como broadcast no switch;

8.8.97. Deve implementar em todas as interfaces do switch o protocolo MLD Snooping (v1 e v2), não permitindo que o tráfego MULTICAST IPv6 seja tratado como broadcast no switch;

8.8.98. Deve implementar IPv6;

8.8.99. Deve permitir a configuração de endereços IPv6 para gerenciamento;

8.8.100. Deve permitir consultas de DNS com resolução de nomes em endereços IPv6;

8.8.101. Deve implementar ICMPv6 com as funcionalidades de ICMP request, ICMP Reply, ICMP Neighbor Discovery Protocol (NDP) e ICMP MTU Discovery;

8.8.102. Deve implementar protocolos de gerenciamento Ping, Traceroute, Telnet, SSH, TFTP, FTP, SNMP, SCP, SYSLOG, HTTP, HTTPS e DNS sobre IPv6;

8.8.103. Deve implementar NTPv4 com suporte a IPv6;

8.8.104. Deve implementar IPv6 MLD snooping v1 e v2;

8.8.105. Deve implementar mecanismo de Dual Stack (IPv4 e IPv6), para permitir migração de IPv4 para IPv6;

8.8.106. Deverá ter suporte a instalações do tipo "plug-and-play" para facilitar a troca de switches;

8.8.107. O switch deve ter a capacidade de identificar, ao menos, pelos seguintes mecanismos MAC, OUI, LLDP, MAB e 8021.X os equipamentos diretamente conectados a qualquer uma das interfaces do dispositivo. Ao identificar este equipamento deve ser capaz de configurar automaticamente a interface a que este equipamento estiver conectado, aplicando desde descrição da porta até as políticas de segurança e qualidade de serviço da mesma;

8.8.108. Deverá ser capaz de identificar o equipamento, rede a que pertence ou em que está autenticado e ser capaz de aplicar o QoS definido para ele de forma automática. Sendo desta forma capaz de associar automaticamente a interface níveis de QoS de voz e vídeo pré-definidos;

8.8.109. O switch deve ser capaz de implementar funcionalidades para visualização de consumo, desabilitando interfaces em horários pré-determinados que estejam alimentando equipamentos;

8.8.110. Deve suportar UniDirectional Link Detection Protocol (UDLD) e Aggressive UDLD para detectar problemas de conexão ou problemas em um cabo de fibra óptica, desativando as portas do switch;

8.8.111. Deve implementar TDR (Time Domain Reflectometer) para detectar, caracterizar e localizar falhas nos cabos metálicos tanto nas interfaces UTP como nas interfaces de duplo propósito.

8.9. ***Solução de Email Gateway*:**

8.9.1. A solução de E-mail *Gateway* Antispam deve ser instalada no *datacenter* principal da Pref. Municipal de Foz do Iguaçu, de modo a prover segurança de e-mail, conforme topologia de rede a ser obtida durante a visita técnica;

8.9.2. A solução deve ser provida por meio de um appliance físico com função de *Gateway* Antispam, Antivirus e Proteção Contra Perda de Dados, de modo a prover filtragem e segurança de e-mail bem como bloqueio de e-mails não solicitados capazes de impactar a produtividade dos colaboradores da prefeitura e degradar o desempenho dos sistemas e redes corporativas, sendo que o conjunto dos requisitos especificados podem ser atendidos por meio de outros equipamentos e *softwares*;

8.9.3. A Solução deve ser do tipo Appliance com Hardware e Software fabricados e fornecidos pelo mesmo fabricante;

8.9.4. Não serão aceitos equipamentos servidores de uso genérico;

8.9.5. Não serão aceitas soluções de Software Livre ou Código Aberto;

8.9.6. A solução deve estar licenciada e operacional para 1000 caixas postais/usuários;

8.9.7. O equipamento não deve ultrapassar altura de 1U e ter dimensões padrão rack 19";

8.9.8. O equipamento deve suportar fontes de alimentação redundantes;

8.9.9. O equipamento deve suportar Remote Power Cycling;

8.9.10. O equipamento deve conter no mínimo 6 interfaces 1G Base-T RJ45 habilitadas e operacionais;

8.9.11. O equipamento deve conter memória RAM do tipo DDR4 com mínimo 16GB de memória instalada;

8.9.12. O equipamento deve conter discos em RAID1;

8.9.13. O equipamento deve conter no mínimo 1.2TB de espaço em disco;

8.9.14. Assim, o elemento com função de Email *Gateway* deve suportar aos seguintes requisitos mínimos:

8.9.14.1. Função de Relay SMTP (*Simple Mail Transfer Protocol*), com recurso de antispam;

8.9.14.2. Função de Outbreak Filter, podendo ser criados filtros ou combinação de pelo menos seis parâmetros, sendo eles: tipo de arquivo, nome do arquivo, tamanho do arquivo e URL contida na mensagem;

8.9.14.3. A Função Outbreak Filter deve permitir a reescrita de URLs contidas em mensagens suspeitas;

8.9.14.4. Capacidade de *throughput* de 500 (quinhentas) conexões SMTP simultâneas;

8.9.14.5. Capacidade de atendimento ao tráfego de e-mail gerado a partir 1000(mil) caixas postais de correio eletrônico da Rede da Prefeitura, com taxa média de 70 (cem) mensagens encaminhadas por hora;

8.9.14.6. Controle de sessões SMTP por meio de limite de tráfego de mensagens baseado em endereços IP, sub-redes IP, domínio e reputação do emissor;

8.9.14.7. Inspeção e bloqueio de mensagens baseados em tamanho de mensagem, volume de mensagens por período, número de destinatários por mensagem, número de destinatários por hora, destinatários inválidos, número de mensagens por conexão e número de conexões simultâneas por endereço IP;

8.9.14.8. Implementação da tecnologia SPF (*Sender Policy Framework*), de modo a evitar que outros domínios enviem e-mails não autorizados em nome de um domínio;

8.9.14.9. Implementação da tecnologia DKIM (*Domain Keys Identified Mail*), de modo a prover mecanismo para autenticação de e-mail baseado em criptografia de chaves públicas;

8.9.14.10. Proteção contra ataques de diretório (*Directory Harvest Attack*), técnica de busca, descoberta e validação de endereços de e-mail no domínio por força bruta;

8.9.14.11. Implementação de recursos de controle de taxa (*E-mail Throttling*), limitando a quantidade de e-mail aceitos de um emissor específico durante um período de tempo;

8.9.14.12. Implementação de recursos de verificação de DNS reverso para validação de domínio;

8.9.14.13. Filtragem de conteúdo de e-mails por meio de assinaturas para corpo e anexos de mensagens, heurística, filtro de reputação, URLs e filtros *anti-phishing*;

8.9.14.14. Filtragem de conteúdo de e-mails, permitindo a concatenação por operações booleanas de regras de expressões regulares nos campos de cabeçalho SMTP, corpo, tamanho e anexos da mensagem;

8.9.14.15. Filtragem de e-mails baseada em lista negra e lista branca, globais e por usuário;

8.9.14.16. Remoção de corpo e anexos de mensagens;

8.9.14.17. Categorização de mensagens de saída a partir de políticas preestabelecidas;

8.9.14.18. Implementação de recurso de antivírus;

8.9.14.19. Tratamento de mensagens com anexos contendo vírus, possibilitando o encaminhamento da mensagem sem o anexo infectado, bloqueio da mensagem e alerta ao destinatário do ocorrido;

8.9.14.20. Detecção de arquivos anexos, baseada em tipo, nome, extensão e formato MIME (*Multipurpose Internet Mail Extensions*);

8.9.14.21. Detecção de anexos criptografados, permitindo definir a ação a ser executada;

8.9.14.22. Detecção de reputação de *links* que estejam dentro do corpo de mensagens;

8.9.14.23. Configuração de sensibilidade de risco de cada mensagem, permitindo definir limites para encaminhamento, tageamento, não aceitação e quarentena de mensagens;

8.9.14.24. Implementação de recurso de quarentena por usuário, integrado e autenticado no *Microsoft Active Directory*;

8.9.14.25. Implementação de recurso de envio de notificação periódica para usuários acerca de mensagens de spam e em quarentena;

8.9.14.26. Implementação de recurso que permita o usuário administrar a sua própria quarentena;

8.9.14.27. Implementação de recurso de cadastro de lista negra e branca pelo próprio usuário;

8.9.14.28. Implementação de configuração para bloqueio, encaminhamento, marcação e quarentena pelo próprio usuário;

8.9.14.29. Implementação de inserção de carimbo no assunto de mensagens e de texto no corpo de mensagens;

8.9.14.30. Implementação de inserção de *header* personalizado (*x-header*);

8.9.14.31. Gerenciamento por CLI (*Command-line interface*), SSH (*Secure Shell*), WebUI (*WEB User Interface*) via HTTPS (*Secure Hypertext Transfer Protocol*) e console gráfica centralizada;

8.9.14.32. Gerenciamento único, centralizado, virtualizável, responsável pela aplicação das políticas de segurança, administração e controle das funcionalidades dos serviços;

8.9.14.33. Gerenciamento por meio de *software* a ser instalado em ambiente virtualizado da prefeitura;

8.9.14.34. Gerenciamento com perfis de acessos distintos para administração de funcionalidades, acesso a *logs* e emissão de relatórios;

8.9.14.35. Gerenciamento com visualização de *status* de serviços;

8.9.14.36. Gerenciamento com recurso de informações estatísticas de fluxo de tráfego, incluindo quantidade de conexões, *throughput* e desempenho dos serviços;

8.9.14.37. Gerenciamento com recurso de auditoria de alteração de configurações e acesso à ferramenta de administração, incluindo usuário, data e horário de acesso e ações realizadas;

8.9.14.38. Gerenciamento com recurso de replicação de configurações e atualização de *software*;

8.9.14.39. Gerenciamento com recurso de monitoramento de *logs* e *debugging*;

8.9.14.40. Gerenciamento com recurso de *backup* e importação de arquivos de configuração;

8.9.14.41. Gerenciamento com recurso de emissão de relatórios, incluindo informações de quantidade de conexões, endereços IP, quantidade de e-mails, quantidade de *spams*, quantidade de vírus, volume de tráfego, performance, processamento e armazenamento;

8.9.14.42. Gerenciamento com recurso de integração e envio automático de *logs* para os serviços referentes ao item 10 – Administração e Monitoramento de Segurança.

8.10. **SOLUÇÃO DE SEGURANÇA DE *WEB*:**

8.10.1. **Do Objeto**

8.10.1.1. A solução ofertada deverá ser robusta, segura e eficiente para proteger o ambiente de navegação à internet, provendo as funcionalidades de:

8.10.1.1.1. *Proxy HTTP, HTTPS e FTP*;

8.10.1.1.2. Caching;

8.10.1.1.3. Categorização e Controle de URL;

8.10.1.1.4. Análise e bloqueio de URLs usando conceito de Reputação;

8.10.1.1.5. Controle e Visibilidade de Aplicações WEB;

8.10.1.1.6. Filtragem de Conteúdo;

8.10.1.1.7. Deve possuir no mínimo 3 modulos internos (engines) de AntiVírus, sendo que as engines de antivírus devem ser obrigatoriamente de fabricantes diferentes;

8.10.1.1.8. Inspeção de Tráfego SSL;

8.10.1.1.9. Módulo de controle AntiMalware com suporte a proteção contra malwares avançados sem a necessidade de inclusão de equipamentos adicionais.

8.10.1.2. A solução fornecida deverá suportar no mínimo, 2.000 mil usuários simultâneos sem necessidade de acréscimo de hardware;

8.10.1.3. A solução deverá estar licenciada e operacional para suportar 2.000 usuários.

8.10.1.4. A solução deve ser do tipo Appliance físico com hardware e software fabricados e fornecidos pelo mesmo fabricante;

8.10.1.5. Não serão aceitos servidores de uso genérico;

8.10.1.6. Não serão aceitas soluções com software livre ou código aberto;

8.10.1.7. O equipamento deve ter altura máxima de 1U com padrão Rack 19";

8.10.1.8. O equipamento deve suportar Remote Power Cycling;

8.10.1.9. O equipamento deve suportar fontes de alimentação redundantes e integradas ao equipamento;

8.10.1.10. O equipamento deve possuir no mínimo 6 interfaces 1G Base-T RJ45 instaladas, habilitadas e operacionais;

8.10.1.11. O equipamento deve possuir memoria RAM do tipo DDR4 com no mínimo 32GB de memória instalada e operacional;

8.10.1.12. O equipamento deve possuir no mínimo 2.4TB de espaço em disco com mirroring RAID-10;

8.10.1.13. A solução fornecida deve ser construída no conceito de appliance físico, contendo software específicos e sistema operacional especializado. Todas as funcionalidades a serem implementadas deverão ser executadas no mesmo equipamento, com exceção à solução de relatórios que poderá ser adicionada em um appliance em paralelo podendo este ser físico ou virtual. Toda a solução de hardware e software deverá ser fornecida pelo mesmo fabricante;

8.10.1.14. A solução deverá suportar alta disponibilidade e deverá funcionar com os seguintes requisitos:

8.10.1.14.1. Um appliance (ou grupo de appliances) deverá ser capaz de suportar toda a demanda de usuários.

8.10.1.14.2. Outro appliance (ou grupo de appliances) deverá prover alta disponibilidade para toda a demanda de usuários.

8.10.2. **CARACTERÍSTICAS DE *PROXY* E *CACHE*:**

8.10.2.1. Servidor Proxy deverá ser compatível para navegação com qualquer browser e sistema operacional;

8.10.2.2. Atuar nativamente como proxy dos protocolos HTTP, HTTPS e FTP;

8.10.2.3. Atuar como proxy SOCKS, com definições de políticas de usuários e grupos específicas para esse protocolo;

8.10.2.4. Para o acesso a GUI (Graphical User Interface) o browser deve suportar e estar habilitado para aceitar JavaScript e cookies;

8.10.2.5. A sessão de administração a GUI deverá expirar o login depois de no minimo 30 minutos de inatividade;

8.10.2.6. Deve suportar no mínimo os seguintes navegadores para o gerenciamento via GUI:

8.10.2.6.1. Firefox 3.0 e versões mais recentes;

8.10.2.6.2. Internet Explorer 7.0 e versões mais recentes - (Windows apenas);

8.10.2.6.3. Safari 4.0 e versões mais recentes - (Mac OS X apenas);

8.10.2.6.4. Google Chrome.

8.10.2.7. A interface de configuração via GUI deve suportar no mínimo os seguintes idiomas:

8.10.2.7.1. Inglês;

8.10.2.7.2. Português Brasil;

8.10.2.7.3. Espanhol.

8.10.2.8. Suportar controle de FTP sobre HTTP (nos modos ativo e passivo);

8.10.2.9. O cliente de FTP pode especificar a porta para controle de conexão através do seguinte formato: hostname:port;

8.10.2.10. Independentemente do modo do FTP client que o usuário utilizar o FTP proxy, o mesmo deverá primeiro tentar atuar no modo passivo a conexão ao

servidor FTP. Caso o servidor remoto não suporte Passive Mode, o Proxy deverá operar em modo ativo;

8.10.2.11. Possibilitar a configuração da porta ou portas utilizadas para o serviço de Proxy para HTTP, HTTPS, FTP e SOCKS;

8.10.2.12. Possuir a capacidade de utilizar o proxy com o método CONNECT para portas tuneladas em HTTP;

8.10.2.13. Deve ser capaz de criar lista de destinos que poderão pular as regras de proxy e políticas baseadas no mínimo em:

8.10.2.13.1. Endereço IP;

8.10.2.13.2. CIDR;

8.10.2.13.3. Domínio;

8.10.2.13.4. Hostname completo ou parte;

8.10.2.13.5. Grupo de usuários;

8.10.2.13.6. Categorias de URL;

8.10.2.13.7. Portas do Proxy.

8.10.2.14. O proxy fornecido deve suportar operação tanto em modo explícito como em modo transparente. No caso de modo transparente, deve ser implementado o redirecionamento de conexões através do protocolo WCCPv2;

8.10.2.15. O serviço de proxy deverá funcionar para IPv4 e IPv6 – em modo transparente e explícito;

8.10.2.16. Possuir integração com serviços de diretório LDAP e domínios Windows para auditoria e autenticação sem a necessidade de instalação de agentes ou plugins em nenhuma estação de trabalho ou servidor;

8.10.2.17. A solução deverá fazer a autenticação do usuário via NTLM de modo transparente, ou seja, utilizando usuário já autenticado em domínio Windows sem pedir novamente a senha para o usuário;

8.10.2.18. O equipamento deve pedir autenticação (login, senha e domínio) para usuários que estejam utilizando sistemas operacionais diferentes do Windows (Linux, por exemplo), validando estes usuários no serviço de diretórios Microsoft Active Directory e LDAP;

8.10.2.19. A solução deverá ser compatível com o padrão Security Assertion Markup Language versão 2(SAMLv2);

8.10.2.20. A solução deverá ter a capacidade de funcionar como um provedor de identidade em ambientes com SAML, criando, mantendo e gerenciando informações de identidade e provendo tais informações a provedores de serviços;

8.10.2.21. Deve ser possível a um usuário com perfil de administrador acessar, a partir de uma máquina de outro usuário, sites e recursos que não estejam disponíveis para tal usuário com menor privilégio;

8.10.2.22. Deverá permitir re-autenticação, onde um usuário com perfil de administrador possa acessar determinados sites/recursos de uma máquina de outro usuário que nao tenha o perfil de acesso;

8.10.2.23. Deverá permitir a criação de políticas com um perfil de Bypass de autenticacao, permitindo que usuários ou visitantes possam acessar a internet com acesso limitado, pelo fato de não ser um usuário autenticado;

8.10.2.24. Deve permitir a criação de políticas sofisticadas usando, no mínimo, os seguintes critérios:

8.10.2.24.1. Grupos do domínio ou serviço de diretórios LDAP e AD aos quais o usuário pertence;

8.10.2.24.2. Classificação das páginas (categorias de URLs);

8.10.2.24.3. Tipos de arquivo;

8.10.2.24.4. Porta do serviço de proxy a que o usuário conectou;

8.10.2.24.5. Reputação do site de destino;

8.10.2.24.6. Listas de URLs cadastradas;

8.10.2.24.7. Base de URLs com contratação de atualizações com o fornecedor;

8.10.2.24.8. Tipo de conteúdo;

8.10.2.24.9. Mime Type;

8.10.2.24.10. Presença de malware;

8.10.2.24.11. Tamanho do download;

8.10.2.24.12. Endereço IP;

8.10.2.24.13. Expressões Regulares para URLs;

8.10.2.24.14. Expressões Regulares para objetos;

8.10.2.25. O sistema deverá ser capaz de hospedar arquivos PAC (Proxy Auto-configuration) e disponibilizá-lo através de portas configuráveis;

8.10.2.26. A solução deverá permitir a reposição do PAC existente com uma nova versão do mesmo nome, e a solução deverá questionar se quer substituir ou não;

8.10.2.27. Deverá ser possível configurar múltiplos Upstream Proxy HTTP afim de redirecionar o trafego se necessário para outras camadas de Proxy,possibilitando configurações de Failover, Balanceamento ou condicional;

8.10.2.28. A solução quando implementada com o recurso de upstream proxy, deverá permitir que o endereço IP seja especificado através do header X-forwarded-for, ao invés de ter somente o endereço IP do downstream proxy;

8.10.2.29. Deve possuir a funcionalidade de IP Spoofing (possibilitar encaminhar o endereço IP do cliente, e não do próprio proxy);

8.10.2.30. A funcionalidade de IP Spoofing deverá ser implementada em conjunto com WCCP (simultaneamente);

8.10.2.31. Permitir roteamento de Proxy baseado em:

8.10.2.31.1. Origem e/ou destino;

8.10.2.31.2. Navegador utilizado no cliente;

8.10.2.31.3. Baseada em um range de tempo específico;

8.10.2.31.4. Porta específicas;

8.10.2.31.5. Categorias de URLs.

8.10.3. **PERFORMANCE**:

8.10.3.1. O equipamento deve suportar no mínimo 2**.000** requisições HTTP por segundo, considerando as configurações mínimas;

8.10.3.2. Possuir capacidade de suportar no mínimo **10.000** conexões TCP simultâneas;

8.10.3.3. Possuir latência de **5 a 15 milissegundos** no máximo;

8.10.3.4. Deve permitir o armazenamento em Cache de conteúdo trafegados pelos usuários que utilizam o serviço de Proxy;

8.10.3.5. Deve possuir a funcionalidade de eliminar o conteúdo do Cache (limpar o Cache);

8.10.3.6. Deve possuir capacidade de criar listas de domínios cujo conteúdo não deve ser armazenado em cachê;

8.10.3.7. Possuir a funcionalidade de listar as URLs, dominios para nunca entrarem em cache;

8.10.3.8. Possuir sistema de arquivos que armazene o conteúdo de cada página em setores contínuos do disco para otimizar o acesso aos objetos armazenados;

8.10.3.9. Cache seguro com varredura completa a cada atualização de vacinas;

8.10.3.10. Possuir espaço em cache para no mínimo 100Gb;

8.10.3.11. Deve permitir a inserção de cabeçalhos customizados (*strings*) nas requisições de conexão a domínios específicos que exijam essa funcionalidade (ex.: YouTube for Schools);

8.10.3.12. Deve permitir a configuração de quotas de volume de tráfego e tempo de uso. As quotas devem permitir o uso de serviços de internet (ou classe de serviços internet) por usuários individualmente, até que se atinja o limite pré-configurado pelo administrador.

8.10.4. **CARACTERÍSTICAS DO PROXY HTTPS (CRIPTOGRAFADO):**

8.10.4.1. A solução deverá possuir a capacidade de decriptografar conexões HTTPS, usando pelo menos os seguintes critérios:

8.10.4.1.1. Baseado na categoria do site de destino;

8.10.4.1.2. Baseado na reputação do site de destino;

8.10.4.1.3. Baseado no status do certificado fornecido pelo site de destino (ex. sites com certificados expirados ou assinados por uma CA não confiável sempre serão descriptografados).

8.10.4.2. A solução deverá permitir a aplicação das mesmas análises efetuadas para os protocolos FTP e HTTP para o protocolo SSL/HTTPS;

8.10.4.3. A solução deverá atuar como um "man in the midle", e deverá suportar certificados on-box, importando certificados válidos ou gerando certificados auto-assinados;

8.10.4.4. A solução deverá suportar a funcionalidade de Requisicao de Assinatura de Certificado – Certificate Signing Request (CSR) Support – ou seja, quando for gerado um certificado e a chave na solucão, deverá permitir que o CSR permita ser submetido em uma CA. E após receber o certificado da CA, o mesmo permita fazer o upload de volta para solucão e esse processo deve ser feito via GUI;

8.10.4.5. Deve suportar módulo de criptografia aderente ao padrão FIPS 140-2, Nível 1;

8.10.4.6. Deve suportar protocolo OCSP (Online Certificate Status Protocol) para verificação em tempo real de status de certificados, junto à autoridade certificadora correspondente;

8.10.4.7. Deve possibilitar a administração de certificados, permitindo a inclusão e remoção de certificados da lista de certificados confiáveis;

8.10.4.8. Deve permitir o upload de certificados com chaves privadas criptografadas, protegidas por senha inacessível aos usuários;

8.10.4.9. Deve suportar chaves de certificados SSL de 2048 bits.

8.10.5. **CARACTERÍSTICAS DO FILTRO DE CONTEÚDO WEB:**

8.10.5.1. O equipamento deve atualizar a base de URLs automaticamente via Internet por meio de uma base proprietária do fabricante do equipamento;

8.10.5.2. Deve possuir uma base de URLs com, no mínimo, 70 categorias pré-definidas, 250.000 de URL's categorizadas e 50 milhões de domínios cadastrados;

8.10.5.3. A base de URLs deve possuir sites em no mínimo 50 línguas e de no mínimo 200 países;

8.10.5.4. Deve permitir a criação de categorias extras customizadas, sem limite, baseadas no mínimo em:

8.10.5.4.1. endereço IP do servidor;

8.10.5.4.2. sub-rede;

8.10.5.4.3. domínio;

8.10.5.4.4. expressões regulares nas URLs.

8.10.5.5. Deve possibilitar o envio ao fabricante das URLs não cadastradas na base de dados para análise e inclusão na base de categorias via appliance e via portal do fabricante;

8.10.5.6. Deve possuir analise de conteúdo dinâmico dos sites permitindo a categorização em tempo real dos sites que não pertencem a nenhuma categoria pré-estabelecida.;

8.10.5.7. Deve permitir notificar o usuário sobre a política de uso da empresa quando acessar sites proibidos, permitindo ou não o acesso se o usuário desejar continuar;

8.10.5.8. A página de notificação para o usuário deverá rastrear quem aceitou a página do "End User Acknoledgement" por sessão do cookie ou endereço IP quando não houver um username disponivel;

8.10.5.9. A solução deverá recordar/armazenar a Informação de Notificação "End User Acknoledgement" mesmo após a reinicialização do proxy;

8.10.5.10. Possuir categoria específica para sites que possam conter malware;

8.10.5.11. Possibilidade de bloqueio de acesso a sites de Chat e fóruns on-line;

8.10.5.12. Possuir categoria específica para sites de download;

8.10.5.13. Possuir categoria específica para sites que tenham como objetivo a distribuição de rádio, vídeo e telefonia pela internet;

8.10.5.14. Deverá ser capaz de criar ações diferentes para as URLs em políticas por tempo;

8.10.5.15. Deverá permitir customização da página de notificações aos usuários;

8.10.5.16. Deve possuir no mínimo as seguintes categorias de URLs, sem custos adicionais:

8.10.5.16.1. Sites de conteúdos maliciosos;

8.10.5.16.2. Site de bate-papo (chat) e fóruns on-line;

8.10.5.16.3. Sites de Filter Avoidances;

8.10.5.16.4. Sites de relacionamento;

8.10.5.16.5. Sites de networking pessoal;

8.10.5.16.6. Sites de Acesso Remoto e Residencial – não permitir acesso a maquinas remotas via URLs dinâmicas e que caracterizem o acesso remoto;

8.10.5.16.7. Sites de pornografia (conteúdo adulto, pedofilia, erótico e também educacao sexual);

8.10.5.16.8. Sites de webmails e de webmail corporativo (OWAs);

8.10.5.16.9. Sites de download e peer-to-peer (P2P);

8.10.5.16.10. Sites de streaming (audio e video on-line);

8.10.5.16.11. Sites de jogos;

8.10.5.16.12. Sites de hacking.

8.10.5.17. Dever possuir filtro contra perda de informações via Web (HTTP e HTTPS) e FTP com no mínimo analisando os seguintes parâmetros. (Ex. Funcionários do Financeiro não pode enviar arqiuvo XLS via FTP):

8.10.5.17.1. Metadata Arquivo (nome do arquivo, tipo do arquivo e tamanho do arquivo);

8.10.5.17.2. Usuário;

8.10.5.17.3. Grupo de usuários (integração AD/LDAP);

8.10.5.17.4. URL, Categoria ou Reputação.

8.10.5.18. Deve permitir integração com DLP (Data Loss Prevention) externo via protocolo ICAP;

8.10.5.19. Deverá conter as seguintes ações:

8.10.5.19.1. Bloquear o site com log do acesso;

8.10.5.19.2. Liberação da página com log do acesso;

8.10.5.19.3. Redirecionar as requisições para uma URL determinada;

8.10.5.19.4. Inspeção profunda (antimalware e inspeção de HTPPS).

8.10.6. **CARACTERÍSTICAS DO FILTRO DE REPUTAÇÃO:**

8.10.6.1. Deve possuir um sistema de filtro de reputação que permita estabelecer uma reputação para cada endereço IP dos servidores de destino com as seguintes características:

8.10.6.2. Deve utilizar dados de uma rede mundial de monitoração de tráfego para definir a reputação dos servidores de destino, consultando um número mínimo de 100.000 redes participantes com cobertura global;

8.10.6.3. A rede de reputação não deve somente ser baseada em informações de fluxo da própria base de Appliances instalada, mas sim em inúmeros outros parâmetros provenientes de: listas negras de URL, listas brancas de URL, listas de equipamentos comprometidos, volume global de trafego, histórico dos sites, dados de categorização de URLs e web crawlers;

8.10.6.4. Deve permitir ações diferenciadas de acordo com cada reputação obtida, como bloquear, permitir ou verificar detalhadamente os objetos de cada acesso.

8.10.7. **CARACTERÍSTICAS DO ANTI-MALWARE:**

8.10.7.1. A solução deverá conter ferramenta anti-malware;

8.10.7.2. Deve suportar o serviço de verificação da reputação de arquivos em nuvem, para detecção preventiva de malwares avançados;

8.10.7.3. A solução deverá permitir, para os casos em que a reputação do arquivo for desconhecida, o envio para análise dinâmica em "Sandbox". Podendo esta análise ser realizada em nuvem ou localmente através da integração com appliances especificos.

8.10.7.4. A solução deverá permitir o acompanhamento da evolução do comportamento de malware para os arquivos análisados, alertando aos administradores os casos em que os arquivos passarem a ter um comportamente malicioso(malware) após análise inicial do serviço de reputação em nuvem;

8.10.7.5. A solução deverá possuir uma base de dados, atualizada periodicamente de forma automática e através do site do fabricante,

8.10.7.6. Efetuar todas as verificações de malware simultaneamente para cada objeto do site, em tempo real, e não seqüencialmente, para minimizar a latência, sem o uso de protocolos de comunicação entre as ferramentas como ICAP;

8.10.7.7. A análise antimalware, deverá ser executada no mesmo equipamento, não sendo aceitas soluções que necessitem de equipamentos adicionais adicional para execução destas funcionalidades;

8.10.7.8. Deve realizar a verificação de malware nos dois sentidos (download e upload);

8.10.7.9. O mecanismo de verificação de malware deve reconhecer códigos maliciosos pelo menos nas seguintes categorias:

8.10.7.9.1. Adware;

8.10.7.9.2. Phishing;

8.10.7.9.3. Trojan Horse;

8.10.7.9.4. Commercial System Monitor;

8.10.7.9.5. Session hijackers;

8.10.7.9.6. Worm;

8.10.7.9.7. Keystrokes – keyloggers;

8.10.7.9.8. Outbreak Heuristic;

8.10.7.9.9. Vírus.

8.10.7.10. Possibilidade de armazenar o resultado das verificações de malware em cache para minimizar a latência;

8.10.7.11. Deve possuir mecanismo de verificação de tráfego na camada 4 do modelo OSI, permitindo identificar estações de trabalho infectadas por malwares na rede interna do cliente, com as seguintes características;

8.10.7.12. A monitoração de tráfego na camada 4 deve examinar o tráfego em todas as 65.535 portas do protocolo TCP;

8.10.7.13. A verificação de tráfego na camada 4 deve ser capaz de apenas monitorar ou monitorar e bloquear o tráfego suspeito;

8.10.7.14. Deverá ser disponibilizado um relatório de gerenciamento de camada 4, integrado ao appliance que exiba e determine os sites e aplicaçoes que foram monitorados/bloqueados;

8.10.7.15. Deverá ser disponibilizado um relatório de gerenciamento de camada 4, integrado ao appliance que exiba e determine os TOP endereços IPs que acessaram sites com malware por portas.

8.10.8. **FUNCIONALIDADE DE ADMINISTRAÇAO E GERENCIA:**

8.10.8.1. Deve possuir interface de gerência via Web e linha de comando;

8.10.8.2. A interface de linha de comando deve ser acessível via protocolo SSH (Secure Shell) e possuir, no mínimo, comandos equivalentes aos seguintes comandos da interface de linha de comando do Linux:

8.10.8.2.1. Tcpdump;

8.10.8.2.2. Grep;

8.10.8.2.3. Tail;

8.10.8.2.4. Ping;

8.10.8.2.5. Telnet.

8.10.8.3. Deve possuir MIB própria para verificação das informações de utilização via SNMP e deve possibilitar o envio de alertas administrativos utilizando e-mails;

8.10.8.4. Possibilitar criar políticas de acesso a interface de gerenciamento baseada em endereço IP e/ou range de IPs que podem acessar o sistema;

8.10.8.5. Deve permitir integração com RADIUS para autenticar usuários no console de gerenciamento da solução;

8.10.8.6. Deve-se ter a opção de mapear todas as contas de RADIUS para o perfil de administrador, ou diferentes contas de RADIUS para diferentes perfis de acesso à console de gerência da solução;

8.10.8.7. A solução deverá permitir a criação de multiplos servidores RADIUS para autenticação de usuários à gerencia;

8.10.8.8. O equipamento deve oferecer a possibilidade de envio de chamado ao suporte do fabricante utilizando comando interno que envie dados sobre a configuração do equipamento e informações de status e logs do equipamento para agilizar o atendimento;

8.10.8.9. A solução deverá permitir que os logs sejam configurados para ser enviado para um servidor externo baseado no tamanho do arquivo ou em horários predefinidos, como de hora em hora, diário, semanal mensal, ou horários customizados;

8.10.8.10. Possibilitar suporte remoto ao equipamento pelo fabricante através de acesso seguro ao equipamento habilitado pelo administrador;

8.10.8.11. Deve possuir pelo menos três classes de usuários, sendo elas administrador (com permissão de alterar configurações, gerenciar usuários e atualizar sistema operacional), operador (com permissão de alterar configurações) e convidado (somente acessar informações de relatório e status do equipamento);

8.10.8.12. A solução deverá exibir uma mensagem na interface gráfica, notificando ao administrador quando existe uma versão do sistema operacional mais nova disponível para ser baixada;

8.10.8.12.1. O appliance deve ser capaz de suportar toda a demanda e atender todos os requisitos do edital, em um único equipamento.

8.10.8.13. Deverá ser compatível com SNMP Traps;

8.10.8.14. Deverá ser compatível com Syslog;

8.10.8.15. A solução deve atualizar todos os mecanismos de checagem de forma regular e automática, efetuando o download de forma incremental;

8.10.8.16. O Administrador poderá manualmente fazer as atualizações.

8.10.9. **CARACTERISTICAS DE RELATORIOS**

8.10.9.1. Deve possuir uma interface Web de geração de relatórios com informações em tempo real, integrada ao equipamento, com as seguintes características;

8.10.9.2. Deve permitir a exportação dos dados dos relatórios para CSV e PDF;

8.10.9.3. Deve possibilitar o agendamento do envio dos relatórios por e-mail;

8.10.9.4. A interface Web de relatórios integrada ao equipamento com informações em tempo real deve ter, no mínimo, os seguintes relatórios:

8.10.9.4.1. Visão do sistema;

8.10.9.4.2. Categorias mais acessadas (10 categorias, pelo menos);

8.10.9.4.3. Usuários com mais acessos (10 usuários, pelo menos);

8.10.9.4.4. Atividades do usuário;

8.10.9.4.5. Detalhes do usuário;

8.10.9.4.6. Detalhes da categoria;

8.10.9.4.7. Detalhes do malware;

8.10.9.4.8. Monitor do filtro de reputação;

8.10.9.4.9. Monitor de tráfego na camada 4 do modelo OSI;

8.10.9.4.10. Uso de banda;

8.10.9.4.11. Banda economizada em função de bloqueios.

8.10.9.5. A solução deve possuir ainda uma interface Web de geração de relatórios para informações que não são de tempo real, não necessariamente integrada ao equipamento appliance, com as seguintes características:

8.10.9.5.1. Deve permitir a exportação dos dados dos relatórios para CSV;

8.10.9.5.2. Deve possibilitar o agendamento do envio dos relatórios por e-mail;

8.10.9.5.3. Deve possibilitar o armazenamento das informações em banco de dados relacional.

8.10.9.6. A interface de relatórios de informações que não são de tempo real deve ter, no mínimo, as seguintes funcionalidades:

8.10.9.6.1. Relatório de sites e categorias acessados (geral e por usuário);

8.10.9.6.2. Relatório de sites bloqueados (geral e por usuário);

8.10.9.6.3. Definição de um intervalo de dia e hora para os relatórios;

8.10.9.6.4. Visão do sistema;

8.10.9.6.5. Sites mais acessados;

8.10.9.6.6. Usuários com mais acessos;

8.10.9.6.7. Atividades do usuário;

8.10.9.6.8. Detalhes do usuário.

8.11. **Roteador de Borda Internet Multi Serviço:**

8.11.1. Pelo menos 500Mbps de capacidade de comutação e expansível até 2Gbps mediante expansão de módulos ou aquisição de licenças ou não expansível com pelo menos 2Gbps de capacidade de comutação;

8.11.2. No máximo 2RU de altura;

8.11.3. Pelo menos 16 GB de RAM para uso pelo data plane;

8.11.4. Pelo menos doze portas 1xGE SFP ou UTP sendo que pelo menos quatro delas sejam otimizadas para uso em WAN;

8.11.5. Suporte aos protocolos de roteamento OSPFv2, RIP v 1 e 2, IGRP e MBGP 4;

8.11.6. Suporte a pelo menos 200.000 (duzentas mil) rotas eBGP;

8.11.7. Suporte a SNMPv2c e SNMPv3;

8.11.8. Suporte a NTP;

8.11.9. Suporte a MPLS e MPLS-VPN (MPLS layer 2 e layer 3 VPN);

8.11.10. Suporte a Multicast: PIM-SM, DVRMP, IGMP v3;

8.11.11. Suporte a GRE (Generic Routing Encapsulation), 8021.q, Ethernet, PPP, MLPPP, PPPoE;

8.11.12. Proteção contra-ataques de SYN *Flood*, UDP *Flood* e IP *Spoofing*;

8.11.13. Suporte a IPFIX ou Netflow;

8.11.14. Capacidade de implementar Policy Based Routing por endereço de origem, porta, interface e também por aplicação e características de QoS (DSCP);

8.11.15. DHCP Server e DHCP Relay;

8.11.16. Suporte a listas de acesso IPv4 e IPv6;

8.11.17. Suporte a QoS:

8.11.17.1. Rate limit;

8.11.17.2. Classes de Serviços (pelo menos quatro classes);

8.11.17.3. Banda máxima;

8.11.17.4. Priority Queuing;

8.11.17.5. Marcação e leitura do campo DSCP do cabeçalho IP;

8.11.17.6. Suporte a Class-Based Weighted Fair Queuing (CBWFQ);

8.11.17.7. Suporte a Weighted Random Early Detection (WRED).

8.11.18. VPN Site-to-Site

8.11.18.1. Pelo menos 200 conexões site-to-site simultâneas;

8.11.18.2. Autenticação MD5 e SHA-1;

8.11.18.3. Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;

8.11.18.4. Algoritmo Internet Key Exchange (IKEv1 e v2);

8.11.18.5. 3DES, AES 128, 192 e 256 (Advanced Encryption Standard);

8.11.18.6. Autenticação via certificado IKE PKI.

8.11.19. SSL VPN:

8.11.19.1. Pelo menos 25 conexões simultâneas (e independente das conexões IPSec VPN).

8.11.20. Habilidade de colocar as interfaces em grupos ou zonas de segurança e definir políticas de tráfego entre as mesmas para simplificação da configuração e proteção do

8.11.21. Habilidade de interceptar as requisições para servidores DNS e analisar/bloquear tais requisições baseado em critérios como reputação ou categorias não permitidas. Essa habilidade pode ser executada em conjunto com uma solução separada ou em nuvem.

8.11.22. Deve suportar os seguintes tipos de NAT:

8.11.22.1. NAT dinâmico (Many-to-1);

8.11.22.2. NAT dinâmico (Many-to-Many);

8.11.22.3. NAT estático (1-to-1);

8.11.22.4. NAT estático (Many-to-Many);

8.11.22.5. NAT estático bidirecional 1-to-1;

8.11.22.6. Tradução de porta (PAT);

8.11.22.7. NAT de Origem;

8.11.22.8. NAT de Destino;

8.11.22.9. Suportar NAT de Origem e NAT de Destino simultaneamente;

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

8.11.22.11. NAT64 e NAT46.

8.11.23. Deve implementar DHCP Server em múltiplas VLANS;

8.11.24. Deve implementar DHCP Option 82;

8.11.25. Deve implementar mecanismo de autenticação para acesso local ou remoto ao equipamento baseada em um Servidor de Autenticação/Autorização do tipo TACACS e RADIUS;

8.11.26. Deve proteger a interface de comando do equipamento através de senha;

8.11.27. Deve implementar o protocolo SSH V2 para acesso à interface de linha de comando;

8.11.28. Deve implementar mecanismos de AAA (Authentication, Authorization e Accounting) com garantia de entrega;

8.11.29. Deve implementar a criptografia de todos os pacotes enviados ao servidor de controle de acesso e não só os pacotes referentes à senha.

8.12. **Solução de Endpoint Security:**

8.12.1. Módulo de proteção anti-malware:

8.12.1.1. Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:

- Windows Server 2003 sp2 (32/64-bit);
- Windows Server 2008 (32/64-bit), Windows Server 2008 R2 (32/64-bit) e Windows 2008 Server Core (32/64-bit) ;
- Windows Server 2012 e Windows Server 2012 R2;
- Windows Server 2016;
- Windows XP sp3 (x86/x64);
- Windows Vista sp2 (x86/x64);
- Windows 7 (x86/x64);
- Windows 8 e 8.1 (x86/x64);
- Windows 10 (x86/x64).

8.12.1.2. Deve disponibilizar evidências de varredura em todas as estações de trabalho, identificando as atualizações de sucesso e as ações de insucesso. Para garantir que os casos de insucesso sejam monitorados para tomada de ações pontuais;

8.12.1.3. Deve possuir uma interface Web em protocolo HTTPS ou MMC que mostre um resumo de atualizações, numero de agentes on-line e alertas de ameaças de ransomware;

8.12.1.4. A console deverá possibilitar a busca pelo endpoint na árvore de computadores usando qualquer os sequintes metodos:

8.12.1.5. IPV4, MAC, metodo de scan, range de ip, IPV6 e versões de componentes;

8.12.1.6. A console deve integrar-se com o Microsoft Active Directory para que os usuários do dominio AD possam administrar a solução de acordo com as permissões configuradas para cada usuário;

8.12.1.7. O produto deverá através do uso de senha impedir a desinstalação não autorizada ou remoção do módulo residente em memória do cliente de antivirus;

8.12.1.8. Deve ser integrada ao Windows Security center, quando utilizado plataforma Microsoft;

8.12.1.9. Deve detectar, analisar e eliminar programas maliciosos, tais como vírus, spyware, worms, cavalos de tróia, key loggers, programas de propaganda, rootkits, phishing, dentre outros;

8.12.1.10. Deve possuir a funcionalidade de adicionar Spyware/Grayware em uma lista de aprovados, possuindo uma base interna dessas;

8.12.1.11. Deve possuir a funcionalidade de dectecar cookies maliciosos;

8.12.1.12. Deve detectar, analisar e eliminar, automaticamente e em tempo real, programas maliciosos em:

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

8.12.1.14. Arquivos executados, criados, copiados, renomeados, movidos ou modificados, inclusive em sessões de linha de comando (DOS ou Shell);

8.12.1.15. Arquivos compactados automaticamente, em pelo menos nos seguintes formatos: zip, exe, arj, mime/uu, Microsoft cab;

8.12.1.16. O scan de arquivos comprimidos deverá ser de no minimo 6 camadas de compressão;

8.12.1.17. O scan de arquivos comprimidos do tipo OLE deverá ser de no minimo 10 camadas de compressão;

8.12.1.18. Arquivos recebidos por meio de programas de comunicação instantânea;

8.12.1.19. Deve detectar e proteger em tempo real a estação de trabalho contra vulnerabilidades e ações maliciosas executadas em navegadores web por meio de scripts em linguagens tais como javascript, vbscript/Activex;

8.12.1.20. Deve possuir detecção heurística de vírus desconhecidos;

8.12.1.21. Deve permitir configurar o consumo de cpu que será utilizada para uma varredura manual ou agendada;

8.12.1.22. Deve permitir diferentes configurações de detecção (varredura ou rastreamento):

8.12.1.23. Em tempo real de arquivos acessados pelo usuário;

8.12.1.24. Em tempo real dos processos em memória, para a captura de programas maliciosos executados em memória, sem a necessidade de escrita de arquivo;

8.12.1.25. Manual, imediato ou programável, com interface gráfica em janelas, personalizável, com opção de limpeza;

8.12.1.26. Por linha-de-comando, parametrizável, com opção de limpeza;

8.12.1.27. Automáticos do sistema com as seguintes opções:

8.12.1.28. Escopo: todos os discos locais, discos específicos, pastas específicas ou arquivos específicos;

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

8.12.1.30. Frequência: horária, diária, semanal e mensal;

8.12.1.31. Exclusões: pastas ou arquivos (por nome e/ou extensão) que não devem ser rastreados;

8.12.1.32. Deve possuir mecanismo de cache de informações dos arquivos já escaneados;

8.12.1.33. Deve possuir cache persistente dos arquivos já escaneados para que nos eventos de desligamento e reinicialização das estações de trabalho e notebooks, a cache não seja descartada;

8.12.1.34. Deve possuir ferramenta de alterações de parâmetros de comunicação entre o cliente antivírus e o servidor de gerenciamento da solução de antivírus;

8.12.1.35. Deve permitir a utilização de servidores locais de reputação para análise de arquivos e URL's maliciosas, de modo a prover, rápida detecção de novas ameaças;

8.12.1.36. Deve ser capaz de aferir a reputação das URL's acessadas pelas estações de trabalho e notebooks de forma a proteger o usuário independente da maneira de como a URL está sendo acessada;

8.12.1.37. Deve ser capaz de detectar variantes de malwares que possam ser geradas em tempo real na memória da estação de trabalho ou notebook, permitindo que seja tomada ação de quarentena a ameaça;

8.12.1.38. Deve ser capaz de bloquear o acesso a qualquer site não previamente analisado pelo fabricante;

8.12.1.39. Deve permitir a restauração de maneira granular de arquivos quarentenados sob suspeita de representarem risco de segurança;

8.12.1.40. Deve permitir em conjunto com a restauração dos arquivos quarentenados a adição automática as listas de exclusão de modo a evitar novas detecções dos arquivos;

8.12.1.41. Deve detectar malwares conhecidos e potenciais ameaças baseados no comportamento;

8.12.1.42. Deve realizar proteção de documentos contra criptografia ou modificação não autorizada ;

8.12.1.43. Deve bloquear processos comuns associados a ransomware;

8.12.1.44. Deverá fornecer informações sobre possiveis canais de infecção de ransomware;

8.12.1.45. Deverá ser possivel monitorar eventos do Sistema Operacional como :

8.12.1.46. Arquivos duplicados, Modificação do arquivo Hosts do Windows, Novos Serviços adicionados, Novo plugin no Internet Explorer, Modificação de processos Do Sistema;

8.12.1.47. As ações do monitoramento de comportamento deverão possuir as seguintes ações:

8.12.1.48. Permitir, bloquear, perguntar quando necessario e apenas log;

8.12.1.49. Sobre o monitoramento de comportamento o mesmo deverá possuir funcionalidade lista de programas bloquedos e liberados;

8.12.1.50. A ferramenta de Antivirus deverá verificar a reputação de arquivos e URLS;

8.12.1.51. A ferramenta de Antivirus deverá possuir a funcionalidade de scan no protocolo POP3;

8.12.1.52. A ferramenta de Antivirus deverá fornecer a proteção contra URLS maliciosas, efetuando o scan de portas e URLS nos procotolos HTTP e HTTPS;

8.12.1.53. A proteção contra URLS maliciosas da solução de Antivirus deverá possuir três niveis se segurança Alto, Medio e baixo além de uma lista para liberar ou bloquear URLS,

8.12.1.54. Deverá dectectar e bloquear conexões suspeitas com C&C além de efetuar o bloqueio do malware que estiver fazendo a conexão;

8.12.1.55. Deverá possibilitar ao administrador adicionar exceções para os endereços ips que foram detectados como suspeitos;

8.12.1.56. Deverá possuir a funcionalidade de Machine Learn para identificar malwares, conexões e processos suspeitos;

8.12.1.57. O log da Machine Learn deverá apresentar um veredicto informando o motivo da dectação e se existe alguma semelhança com algum malware já conhecido.

8.12.1.58. Devera possuir proteção Anti-exploit para detectar e bloquear ameaças usando CVE (Common Vulnerabilities and Exposures);

8.12.1.59. Deverá escanear o setor boot de dispositivos USB depois que o mesmo for plugado na estação;

8.12.1.60. Deverá possuir a funcionalidade de detectar códigos com exploit em arquivos OLE.

8.12.2. Funcionalidade de atualização:

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

8.12.2.2. Deve permitir atualização incremental da lista de definições de vírus;

8.12.2.3. Deve permitir a atualização automática do engine do programa de proteção a partir de localização na rede local ou na internet, a partir de fonte autenticável;

8.12.2.4. Deve permitir o rollback das atualizações das listas de definições de vírus e engines;

8.12.2.5. Deve permitir a indicação de agentes para efetuar a função de replicador de atualizações e configurações, de forma que outros agentes possam utiliza-los como fonte de atualizações e configurações, não sendo necessária a comunicação direta com o servidor de anti-malware para essas tarefas;

8.12.2.6. Deve permitir que os agentes de atualização possam replicar os componentes de vacinas, motores de escaneamento, versão de programas, hotfix e configurações específicas de domínios da árvore de gerenciamento;

8.12.2.7. O servidor da solução de anti-malware, deve ser capaz de gerar localmente versões incrementais das vacinas a serem replicadas com os agentes replicadores de atualizações e configurações, de maneira a reduzir o consumo de banda necessário para execução da tarefa de atualização;

8.12.2.8. O agente replicador de atualizações e configurações, deve ser capaz de gerar localmente versões incrementais das vacinas a serem replicadas com os demais agentes locais, de maneira a reduzir o consumo de banda necessário para execução da tarefa de atualização;

8.12.2.9. Devera possuir a capacidade de retomar atualizações de vacinas e de software do ponto onde foram interrompidas em caso de perda de conexão, sem necessidade de reinicio de todo o processo.

8.12.3. Funcionalidade de administração:

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

8.12.3.2. Deve possuir a capacidade de armazenar os eventos em banco de dados padrão SQL;

8.12.3.3. Deve possibilitar instalação "silenciosa";

8.12.3.4. Deve permitir o bloqueio por nome de arquivo;

8.12.3.5. Deve permitir o travamento de pastas e diretórios;

8.12.3.6. Deve permitir o travamento de compartilhamentos;

8.12.3.7. Deve permitir o rastreamento e bloqueio de infecções;

8.12.3.8. Deve possuir mecanismo de detecção de ameaças baseado em comportamento de processos que estão sendo executados nas estações de trabalho e notebooks;

8.12.3.9. Deve efetuar a instalação remota nas estações de trabalho, sem requerer outro software ou agente adicional, previamente instalado e sem necessidade de reiniciar a estação de trabalho;

8.12.3.10. Deve desinstalar automática e remotamente a solução de antivírus atual, sem requerer outro software ou agente;

8.12.3.11. Deve permitir a desinstalação através da console de gerenciamento da solução;

8.12.3.12. Deve ter a possibilidade de exportar/importar configurações da solução através da console de gerenciamento;

8.12.3.13. Deve ter a possibilidade de backup da base de dados da solução através da console de gerenciamento;

8.12.3.14. Deve ter a possibilidade de designação do local onde o backup automático será realizado;

8.12.3.15. Deve permitir realização do backup da base de dados através de mapeamento de rede controlado por senha;

8.12.3.16. Deve ter a possibilidade de determinar a capacidade de armazenamento da área de quarentena;

8.12.3.17. Deve permitir a deleção dos arquivos quarentenados;

8.12.3.18. Deve permitir remoção automática de clientes inativos por determinado período de tempo;

8.12.3.19. Deve permitir integração com Active Directory para acesso a console de administração;

8.12.3.20. Identificar através da integração com o Active Directory, quais máquinas estão sem a solução de anti-malware instalada;

8.12.3.21. Deve permitir criação de diversos perfis e usuários para acesso a console de administração;

8.12.3.22. Deve permitir que a solução utilize consulta externa a base de reputação de sites integrada e gerenciada através da solução de anti-malware, com opção de configuração para estações dentro e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante;

8.12.3.23. Deve permitir agrupamento automático de estações de trabalho e notebooks da console de gerenciamento baseando-se no escopo do Active Directory ou IP;

8.12.3.24. Deve permitir criação de subdomínios consecutivos dentro da árvore de gerenciamento;

8.12.3.25. A console de Administração deverá prover um dashboard com a quantidade de ameaças conhecidas, desconhecidas e violações de políticas;

8.12.3.26. O dashboard deverá ser personalizavel permitindo ao administrador adicionar widgets e atalhos como favoritos para facilitar administração;

8.12.3.27. Deve possuir solução de reputação de sites local para sites já conhecidos como maliciosos integrada e gerenciada através da solução de antivírus, com opção de configuração para estações dentro e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante;

8.12.3.28. Deve registrar no sistema de monitoração de eventos da console de anti-malware informações relativas ao usuário logado no sistema operacional

8.12.3.29. Deve prover ao administrador relatório de conformidade do status dos componentes, serviços, configurações das estações de trabalho e notebooks que fazem parte do escopo de gerenciamento da console de antivírus;

8.12.3.30. Deve prover ao administrador informações sobre quais estações de trabalho e notebooks fazem parte do escopo de gerenciamento da console de anti-malware não realizaram o escaneamento agendado ou o escaneamento demandado pelo administrador no período determinado de dias;

8.12.3.31. Possibilitar postegar o scan quando o endpoint estiver usando uma conexão wifi, afim de otimizar o uso de bateria;

8.12.3.32. Deve prover segurança através de SSL para as comunicações entre o servidor e a console de gerenciamento web;

8.12.3.33. Deve prover segurança para as comunicações entre o servidor e os agentes de proteção usando criptografia avançada AES 256;

8.12.3.34. Deve suportar múltiplas florestas e domínios confiáveis do Active Directory;

8.12.3.35. Deve utilizar de chave de criptografia que seja/esteja em conformidade com o Active Directory para realizar uma conexão segura entre servidor de antivírus e o controlador de domínio;

8.12.3.36. Deve permitir a criação de usuários locais de administração da console de anti-malware;

8.12.3.37. Deve possuir a integração com o Active Directory para utilização de seus usuários para administração da console de anti-malware;

8.12.3.38. Deve permitir criação de diversos perfis de usuários que permitam acessos diferenciados e customizados a diferentes partes da console de gerenciamento;

8.12.3.39. Deve bloquear acessos indevidos a área de administração do agente que não estejam na tabela de políticas definidas pelo administrador;

8.12.3.40. Deve se utilizar de mecanismo de autenticação da comunicação entre o servidor de administração e os agentes de proteção distribuídos nas estações de trabalho e notebooks;

8.12.3.41. Deve permitir a gerência de domínios separados para usuários previamente definidos;

8.12.3.42. Deve ser capaz de enviar notificações específicas aos respectivos administradores de cada domínio definido na console de administração;

8.12.3.43. Deve permitir configuração do serviço de reputação de sites da web em pelo menos 3 níveis: baixo, médio e alto;

8.12.3.44. Deve permitir a emissão de alertas via smtp, snmp e gravação de logs no Event Viewer do Windows;

8.12.3.45. Deve possuir sistema de reparação automático para danos caudados por malwares;

8.12.3.46. Possibilitar a distribuição de imagens do antivirus, sendo criados números de identificação únicos para cada imagem gerada prevenindo a duplicação de identificadores;

8.12.3.47. Permitir o agendamento para a verificação de comunicação entre servidor e agente ;

8.12.3.48. Permitir o agrupamento automático do agente por IP ou Active Directory;

8.12.3.49. Funcionar tanto no ambiente corporativo como em VPN;

8.12.3.50. Deverá possuir uma funcionalidade ou feature de relay para que as máquinas que estão fora da rede enviem informações do status do agente, pattern e log;

8.12.3.51. Deverá possuir a funcionalidade para a criação de regras diferentes para estações que estão na rede interna e fora da rede;

8.12.3.52. Deverá possuir ferramentas para que o administrador consiga migrar e exportar as configurações atuais do servidor para outro em caso de migração.

8.12.4. Módulo Funcionalidade de controle de dispositivos:

8.12.4.1. Deve possuir controle de acesso a discos removíveis reconhecidos como dispositivos de armazenamento em massa através de interfaces USB e outras, com as seguintes opções: acesso total, leitura e escrita, leitura e execução, apenas leitura e listar apenas o conteudo;

8.12.4.2. Deve possuir o controle de acesso a drives de mídias de armazenamento como cdrom, dvd, com as opções de acesso total, leitura e escrita, leitura e execução, apenas leitura e bloqueio total;

8.12.4.3. Deve possuir o controle a drives mapeados com as seguintes opções: acesso total, leitura e escrita, leitura e execução, apenas leitura e bloqueio total;

8.12.4.4. Deve permitir escaneamento dos dispositivos removíveis e periféricos (USB, disquete, cdrom) mesmo com a política de bloqueio total ativa.

8.12.5. Módulo Proteção de Vulnerabilidades:

8.12.5.1. Precisa ter a capacidade de detectar e bloquear qualquer conexão indesejada que tente explorar vulnerabilidades do SO e demais aplicações;

8.12.5.2. Precisa ter a capacidade de varrer o servidor protegido detectando o tipo e versão do SO, detectando também as demais aplicações, que blindem vulnerabilidades existentes no SO e aplicações. Esta varredura deverá poder ser executada sob demanda ou agendada;

8.12.5.3. Precisa conter regras de defesa para blindagem de vulnerabilidades e ataques que explorem os seguintes sistemas operacionais: Windows 2000, 2003, 2008, XP, Windows 7, Windows 8 e Windows 10 além de regras para aplicações padrão de mercado, incluindo Adobe Acrobat, Mozilla Firefox, Microsoft Internet Explorer, Google Chrome e Java;

8.12.5.4. As regras de blindagem contra vulnerabilidades deverão conter links com referências externas, isto quando aplicável, explicando a vulnerabilidade do fabricante ou CVE relacionado;

8.12.5.5. Deverá possuir integração com a solução de Endpoint Security para facilitar o gerenciamento e instalação dos agentes.

8.12.6. Funcionalidade de IDS – Host IDS e Host Firewall:

8.12.6.1. Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:

- Windows Server 2003 sp2 (32/64-bit);
- Windows Server 2008 (32/64-bit), Windows Server 2008 R2 (32/64-bit) e Windows 2008 Server Core (32/64-bit) ;
- Windows Server 2012 e Windows Server 2012 R2;
- Windows Server 2016
- Windows XP sp3 (x86/x64);
- Windows Vista (x86/x64);
- Windows 7 (x86/x64);
- Windows 8 e 8.1 (x86/x64);

- Windows 10 (x86/x64).

8.12.6.2. O modulo de IDS deverá prevenir contra os seguintes tipos de ataque :

- Too Big Fragment, Ping da morte, Conflito de ARP, SYN Flood, Overlapping Fragment, Teardrop, Tiny Fragment Attack, Fragmented IGMP e Land Attack.

8.12.6.3. Todas as regras das funcionalidades de firewall e ips de host devem permitir apenas detecção (log) ou prevenção (bloqueio);

8.12.6.4. Deve permitir ativar e desativar o produto sem a necessidade de remoção;

8.12.6.5. O modulo de Host Firewall deverá realizar os seguintes filtros:

8.12.6.6. Inbound/outbound , protocolos (tcp/udp,icmp/icmpv6), portas de destino e origem e destino dos endpoints;

8.12.6.7. A funcionalidade de host Firewall deve possuir regras para controle do tráfego de pacotes de determinadas aplicações;

8.12.6.8. Deve permitir a criação de políticas de segurança personalizadas;

8.12.6.9. Deve permitir configuração e manipulação de políticas de firewall através de prioridades;

8.12.6.10. Deve permitir que o usuário altere as configurações de níveis de segurança e exceções;

8.12.6.11. As exceções do Firewall poderão ser baseadas em aplicações, direções, chaves de registro,protocolos, ranges e endereços ips.

8.12.6.12. Deverá possuir a possibilidade de configurar níveis diferentes de segurança podendo ser eles Alto, médio e baixo;

8.12.6.13. O módulo de Firewall deverá usar o mesmo agente de Anti-virus.

8.12.7. Módulo de proteção anti-malware para estações Linux:

8.12.7.1. Distribuições homologadas pelo fabricante:

- Suse linux enterprise 10,11 e 12;
- Red Hat Enterprise Linux 4.0, 5.0,6.0 e 7.0;
- Centos 4.0, 5.0, 6.0 e 7.0.

8.12.7.2. O agente deve possuir código aberto possibilitando assim adequação a qualquer kernel e distribuição linux, incluindo desenvolvidas ou alteradas internamente e para versões não homologadas pelo fabricante;

8.12.7.3. Varredura manual com interface gráfica, personalizável, com opção de limpeza dos malwares encontrados;

8.12.7.4. Varredura manual por linha de comando, parametrizável e com opção de limpeza automática em todos os sistemas operacionais;

8.12.7.5. Capacidade de detecção e remoção de todos os tipos de malware, incluindo spyware, adware, grayware, cavalos de tróia, rootkits, e outros;

8.12.7.6. Detecção e remoção de códigos maliciosos de macro do pacote Microsoft office, em tempo real;

8.12.7.7. O cliente da solução deve armazenar localmente, e enviar para o servidor (para fins de armazenamento) logs de ocorrência de ameaças, contendo no

mínimo os seguintes dados: nome da ameaça, caminho do arquivo comprometido (quando disponível), data e hora da detecção, endereço ip do cliente e ação realizada;

8.12.7.8. Geração de cópia de segurança dos arquivos comprometidos antes de realizar o processo de remoção de ameaças. Esta cópia deve ser gravada na máquina local, e o acesso ao arquivo deve ser permitido somente pela solução de segurança ou o administrador;

8.12.7.9. A desinstalação do cliente nas estações de trabalho deverá ser completa, removendo arquivos, entradas de registro e configurações, logs diversos, serviços do sistema operacional e quaisquer outros mecanismos instalados;

8.12.7.10. Possibilidade de rastrear ameaças em arquivos compactados em, no mínimo, 15 níveis recursivos de compactação;

8.12.7.11. As mensagens exibidas aos usuários devem ser traduzidas para o português do brasil;

8.12.7.12. Possuir integração com a Console de Gerenciamento Central para envio de informações de ameaças.

8.12.8. Módulo de proteção anti-malware para estações mac-os:

8.12.8.1. O cliente para instalação deverá possuir compatibilidade com os sistemas operacionais:

- Mac os x Lion 10 7.5.8 64 bits;
- Mac os x 10.8 (Mountain Lion) em processadores 32 e 64 bits;
- Mac os x 10.9 Mavericks em processadores 32 e 64 bits;
- Mac os x 10.10 Yosemite em processadores 32 e 64 bits;
- Mac os 10.11 El Capitan em processadores 32 e 64 bits;
- Mac os 10.12 Sierra em processadores 32 e 64 bits.

8.12.8.2. Suporte ao apple remote desktop para instalação remota da solução;

8.12.8.3. Gerenciamento integrado à console de gerência central da solução;

8.12.8.4. Proteção em tempo real contra vírus, trojans, worms, cavalos-de-tróia, spyware, adwares e outros tipos de códigos maliciosos;

8.12.8.5. Permitir a verificação das ameaças em real time, manual e agendada;

8.12.8.6. Permitir a criação de listas de exclusões para pastas e arquivos que não serão verificados pelo antivírus;

8.12.8.7. Permitir a ações de reparar arquivo ou colocar em quarentena em caso de infeções a arquivos;

8.12.8.8. Permitir habilitar scan-cache para otimizar a performance;

8.12.8.9. Possuir a verificação de URL's maliciosas para agentes internos e externos da rede;

8.12.8.10. Possuir a funcionalidade de Certified Safe Software para verificar se um software é legitimo;

8.12.8.11. Deve possuir mecanismo de proteção contra uso não autorizado no qual o agente do antivírus deve ser protegido contra mudança do seu estado (não

possibilitar que um administrador da estação de trabalho e notebook possa parar o serviço do antivírus) bem como mecanismo para restaurar seu estado normal;

8.12.8.12. Deve possuir no mecanismo de autoproteção as seguintes proteções:

8.12.8.13. Autenticação de comandos ipc;

8.12.8.14. Proteção e verificação dos arquivos de assinatura;

8.12.8.15. Proteção dos processos do agente de segurança;

8.12.8.16. Proteção das chaves de registro do agente de segurança;

8.12.8.17. Proteção do diretório de instalação do agente de segurança.

8.12.9. Funcionalidade de HIPS – Host IPS e Host Firewall:

8.12.9.1. Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:

- Windows Server 2003 sp2 (32/64-bit);
- Windows Server 2008 (32/64-bit) e Windows Server 2008 r2 (32/64-bit);
- Windows Server 2012 (32/64-bit);
- Windows XP sp2 / sp3 (x86/x64);
- Windows vista (x86/x64);
- Windows 7 (x86/x64);
- Windows 8 e 8.1 (x86/x64);
- Windows 10 (x86/x64).

8.12.9.2. Deve possuir módulo para proteção de vulnerabilidades com as funcionalidades de host ips e host firewall;

8.12.9.3. Todas as regras das funcionalidades de firewall e ips de host devem permitir apenas detecção (log) ou prevenção (bloqueio);

8.12.9.4. Deve permitir ativar e desativar o produto sem a necessidade de remoção;

8.12.9.5. Deve permitir a varredura de portas logicas do sistema operacional para identificar quais estejam abertas e possibilitando trafego de entrada ou saída

8.12.9.6. A funcionalidade de host ips deve possuir regras para controle do tráfego de pacotes de determinadas aplicações;

8.12.9.7. Deve prover proteção contra as vulnerabilidades do sistema operacional Windows XP ou superior, por meio de regras de host ips;

8.12.9.8. Deve efetuar varredura de segurança automática ou sob demanda que aponte vulnerabilidades de sistemas operacionais e aplicações e atribua automaticamente as regras de host ips para proteger a estação de trabalho ou notebook contra a possível exploração da vulnerabilidade;

8.12.9.9. A varredura de segurança deve ser capaz de identificar as regras de host ips que não são mais necessárias e desativá-las automaticamente;

8.12.9.10. Deve prover proteção contra as vulnerabilidades de aplicações terceiras, por meio de regras de host ips, tais como oracle java, abobe pdf reader, adobe flash player, realnetworks real player, Microsoft office, apple itunes, apple quick time, apple safari, google chrome, mozilla firefox, opera browser, ms internet explorer, entre outras;

8.12.9.11. Deve permitir a criação de políticas diferenciadas em múltiplas placas de rede no mesmo sistema operacional;

8.12.9.12. Deve permitir a criação de políticas de segurança personalizadas;

8.12.9.13. Deve permitir limitar o número de conexões simultâneas no sistema operacional

8.12.9.14. Deve permitir a emissão de alertas via smtp e snmp;

8.12.9.15. Deve permitir configuração e manipulação de políticas de firewall através de prioridades;

8.12.9.16. Deve permitir criação de regras de firewall utilizando os seguintes protocolos:

8.12.9.17. Icmp, icmpv6, igmp, ggp, tcp, pup, udp, idp, nd, raw, tcp+udp.

8.12.9.18. Deve permitir criação de regras de firewall por origem de ip ou mac ou porta e destino de ip ou mac ou porta;

8.12.9.19. Deve permitir a criação de regras de firewall pelos seguintes frame types:

8.12.9.20. Ip, ipv4, ipv6, arp, revarp.

8.12.9.21. Deve permitir também escolher outros tipos de frame type de 4 dígitos em hex code;

8.12.9.22. Deve permitir a criação de grupos lógicos através de lista de ip, mac ou portas;

8.12.9.23. Deve permitir a criação de contextos para a aplicação para criação de regras de firewall;

8.12.9.24. Deve permitir o isolamento de interfaces de rede, possibilitando o funcionamento de uma interface por vez;

8.12.9.25. Deve permitir a criação de múltiplos painéis (dashboards) personalizáveis, compostos por blocos de informações (widgets), visualizados através de gráficos ou tabelas;

8.12.9.26. Os blocos de informações pertencentes aos painéis personalizáveis devem permitir filtros personalizados para facilitar a visualização e gerenciamentos;

8.12.9.27. A seleção de uma informação específica dentro de um bloco de informações, através de um clique, deve redirecionar ao log detalhado que gerou aquela informação;

8.12.9.28. Deve possuir integração com a solução de Antivirus para facilitar o gerenciamento e criação de políticas.

8.12.10. Módulo para controle de aplicações:

8.12.10.1. Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:

- Windows Server 2003 sp2 (32/64-bit);
- Windows Server 2008 (32/64-bit) e Windows Server 2008 r2 (32/64-bit);
- Windows Server 2012 e Windows Server 2012 R2;
- Windows Server 2016;
- Windows XP sp3 (x86/x64);
- Windows XP sp2 (x64);

- Windows Embedded Xpe;
- Windows Embedded POSReady 2009
- Windows Embedded Standard 2009
- Windows 7 (x86/x64);
- Windows Embedded POSReady 7;
- Windows Embedded Standard 7;
- Windows 8 e 8.1 (x86/x64);
- Windows 10 (x86/x64).

8.12.10.2. Deve permitir a criação de políticas de segurança personalizadas;

8.12.10.3. As políticas de segurança devem permitir a seleção dos alvos baseados nos seguintes critérios:

- Nome parcial ou completo das estações de trabalho, permitindo a utilização de caractere coringa para identificação do nome parcial da máquina;
- Range de endereços IPS;
- Sistema operacional;
- Grupos de máquinas espelhados do Active Directory;
- Usuários ou grupos do Active Directory.

8.12.10.4. As políticas de segurança devem permitir a combinação lógica dos critérios para identificação do(s) alvo(s) de cada política;

8.12.10.5. As políticas de segurança devem permitir a definição dos logs que serão recebidos de acordo com os seguintes critérios:

- Nenhum;
- Somente bloqueios;
- Somente regras específicas;
- Todas as aplicações executadas.

8.12.10.6. As políticas de segurança devem permitir o controle do intervalo de envio dos logs;

8.12.10.7. As políticas de segurança devem permitir o controle do intervalo para envio de atualização de cada política;

8.12.10.8. As políticas de segurança devem permitir a definição de qual servidor de gerenciamento o agente de segurança deverá comunicar-se;

8.12.10.9. As políticas de segurança devem permitir a ocultação do ícone do agente, que reside da barra de tarefas, e de notificações ao usuário;

8.12.10.10. As políticas de segurança devem permitir o controle do intervalo de quando os inventários de aplicações são executados;

8.12.10.11. As políticas de segurança devem permitir o controle através de regras de aplicação;

8.12.10.12. As regras de controle de aplicação devem permitir as seguintes ações:

- Permissão de execução;
- Bloqueio de execução;
- Bloqueio de novas instalações.

8.12.10.13. As regras de controle de aplicação devem permitir o modo de apenas coleta de eventos (logs), sem a efetivação da ação regra;

8.12.10.14. As regras de controle de aplicação devem permitir os seguintes métodos para identificação das aplicações:

8.12.10.15. Assinatura sha-1 do executável;

8.12.10.16. Atributos do certificado utilizado para assinatura digital do executável;

8.12.10.17. Caminho lógico do executável;

8.12.10.18. Base de assinaturas de certificados digitais válidos e seguros;

8.12.10.19. As regras de controle de aplicação devem possuir categorias de aplicações;

8.12.10.20. As políticas de segurança devem permitir a utilização de múltiplas regras de controle de aplicações.

8.12.10.21. Deve permitir a criação de múltiplos painéis (dashboards) personalizáveis, compostos por blocos de informações (widgets), visualizados através de gráficos ou tabelas;

8.12.10.22. Os blocos de informações pertencentes aos painéis personalizáveis devem permitir filtros personalizados para facilitar na visualização e gerenciamentos;

8.12.10.23. A seleção de uma informação específica dentro de um bloco de informações, através de um clique, deve redirecionar ao log detalhado que gerou aquela informação;

8.12.10.24. Deve possuir a funcionalidade de instalação remota do agente usando a mesma comunicação do Anti-virus.

8.12.11. Módulo de proteção contra vazamento de informações – DLP:

8.12.11.1. Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:

- Windows Server 2003 sp2 (32/64-bit);
- Windows Server 2008 (32/64-bit), Windows Server 2008 R2 (32/64-bit) e Windows 2008 Server Core (32/64-bit) ;
- Windows Server 2012 e Windows Server 2012 R2;
- Windows Server 2016
- Windows XP sp3 (x86/x64);
- Windows Vista sp2 (x86/x64);
- Windows 7 (x86/x64);
- Windows 8 e 8.1 (x86/x64);
- Windows 10 (x86/x64).

8.12.11.2. Deve possuir nativamente templates para atender as seguintes regulamentações:

- PCI/DSS;
- HIPAA;
- Glba;
- SB-1386;
- US PII.

8.12.11.3. Deve ser capaz de detectar informações, em documentos nos formatos:

- Documentos Microsoft office (doc, docx, xls, xlsx, ppt, pptx) openoffice, rtf, wordpad, text; xml, html;
- Gráficos: visio, postscript, pdf, tiff;

- Comprimidos: win zip, rar, tar, jar, arj, 7z, rpm, cpio, gzip, bzip2, unix/linux zip, lzh;
- Códigos: c/c++, java, verilog, AutoCAD.

8.12.11.4. Deve ser capaz de detectar informações, com base em:

- Dados estruturados, como dados de cartão de crédito, dados pessoais, endereços de e-mail, CPF, entre outros;
- Palavras ou frases configuráveis;
- Expressões regulares;
- Extensão dos arquivos.

8.12.11.5. Deve ser capaz de detectar em arquivos compactados;

8.12.11.6. Deve permitir a configuração de quantas camadas de compressão serão verificadas;

8.12.11.7. Deve permitir a criação de modelos personalizados para identificação de informações;

8.12.11.8. Deve permitir a criação de modelos com base em regras e operadores lógicos;

8.12.11.9. Deve possuir modelos padrões;

8.12.11.10. Deve permitir a importação e exportação de modelos;

8.12.11.11. Deve permitir a criação de políticas personalizadas

8.12.11.12. Deve permitir a criação de políticas baseadas em múltiplos modelos;

8.12.11.13. Deve permitir mais de uma ação para cada política, como:

- Apenas registrar o evento da violação;
- Bloquear a transmissão;
- Gerar alertar para o usuário;
- Gerar uma notificação para o usuário para que ele justique o envio da informação;
- Gerar alertar na central de gerenciamento;
- Capturar informação para uma possível investigação da violação.

8.12.11.14. Deve permitir criar regras distintas com base se a estação está fora ou dentro da rede;

8.12.11.15. Deve ser capaz de identificar e bloquear informações nos meios de transmissão:

- Cliente de e-mail;
- Protocolos http, https, ftp;
- Mídias removíveis;
- Discos óticos cd/dvd;
- Gravação cd/dvd;
- Aplicações de mensagens instantâneas;
- Tecla de print screen;
- Aplicações p2p;
- Área de transferência do Windows;
- Webmail;
- Armazenamento na nuvem (cloud);
- Impressoras;
- Scanners;

- Compartilhamentos de arquivos;
- Activesync;
- Criptografia PGP;
- Portas com, lpt, firewire (ieee 1394);
- Modems;
- Infravermelho;
- Bluetooth.

8.12.11.16. Deve permitir a criação de exceções nas restrições dos meios de transmissão;

8.12.11.17. Deve permitir o scan de metadados de arquivos.

8.12.12. Módulo de criptografia:

8.12.12.1. Deve ser capaz de realizar a criptografia nos seguintes sistemas operacionais:

- Windows XP sp3 (x86/x64);
- Windows Vista SP1 (x86/x64);
- Windows 7 (x86/x64);
- Windows 8 e 8.1 (x86/x64);
- Windows 10 (x86/x64).

8.12.12.2. Deve possuir módulo de criptografia para as estações de trabalho (desktops e notebooks), com as seguintes funcionalidades de criptografia para:

- Disco completo (fde – full disk encryption);
- Pastas e arquivos;
- Mídias removíveis;
- Disco Rígido.

8.12.12.3. Deve possuir autenticação durante a inicialização (boot) da estação de trabalho, antes do carregamento do sistema operacional, para a funcionalidade de criptografia do disco completo;

8.12.12.4. A autenticação durante a inicialização (boot) deve ser a partir das credenciais sincronizadas com o Active Directory;

8.12.12.5. Deve possuir suporte ao algoritmo de criptografia aes-256;

8.12.12.6. Deve possuir a capacidade de exceções para criptografia automática;

8.12.12.7. Deve possuir criptografia no canal de comunicação entre as estações de trabalho e o servidor de políticas;

8.12.12.8. Deve possuir certificação FIPS 140-2;

8.12.12.9. Deve possuir funcionalidade de criptografia por software ou hardware;

8.12.12.10. Deve ser compatível com os padrões SED ('self-encrypting drive), opal e opal2

8.12.12.11. Deve possuir compatibilidade de autenticação por múltiplos fatores;

8.12.12.12. Deve permitir atualizações do sistema operacional mesmo quando o disco está criptografado;

8.12.12.13. Deve possuir a possibilidade de configurar senha de administração local na estação de trabalho para desinstalação do módulo;

8.12.12.14. Deve possuir políticas por usuários, grupos e dispositivos;

8.12.12.15. Deve possuir os métodos de autenticação seguintes para desbloquear um disco:

- Sequência de cores;
- Autenticação com ad;
- Single sign-on com ad;
- Senha pré-definida;
- Número pin;
- Smart card.

8.12.12.16. Deve possuir auto ajuda para usuários que esquecerem a senha com a combinação de perguntas e respostas;

8.12.12.17. Deve possuir mecanismos de criptografia transparentes para o usuário;

8.12.12.18. Deve possuir mecanismos para wipe (limpeza) remoto;

8.12.12.19. Deve possuir mecanismo para desativar temporariamente a autenticação de pré-inicialização (boot);

8.12.12.20. Deve possuir mecanismo que permita desfazer a criptografia do disco no evento em que se torne corrompido, impedindo a inicialização da estação/notebook;

8.12.12.21. O ambiente de autenticação pré-inicialização deve permitir a conexão a redes sem fio (wireless);

8.12.12.22. Deve ser possível especificar o tipo de autenticação das redes wireless disponíveis;

8.12.12.23. O ambiente de autenticação pré-inicialização deve conter indicação visual do estado de conectividade de rede da estação/notebook;

8.12.12.24. O ambiente de autenticação deve disponibilizar um teclado virtual na tela do dispositivo, independente do teclado físico;

8.12.12.25. O ambiente de autenticação pré-inicialização deve permitir a mudança do lay-out do teclado;

8.12.12.26. O ambiente de autenticação pré-inicialização deve prover um mecanismo de assistência remota que permita a autenticação da estação de trabalho no evento que o usuário não se lembre de sua senha de autenticação;

8.12.12.27. O ambiente de autenticação pré-inicialização deve prover um mecanismo que permita a substituição da senha e outros códigos de autenticação através da resposta correta a perguntas definidas previamente pelo administrador;

8.12.12.28. Ambiente de autenticação pré-inicialização deve prover uma ferramenta que permita a execução de procedimentos de identificação de problema, assim como a realização das seguintes tarefas administrativas: desfazer a criptografia do disco, restaurar o registro mestre de inicialização (mbr – master boot record) ao estado anterior ao estado alterado pelo ambiente de autenticação pré-inicialização, montar partições criptografadas, modificar a política de criptografia aplicada à estação de trabalho, adicionar, remover e editar atributos dos usuários existentes na lista de usuários permitidos a se autenticar na estação de trabalho, visualizar os registros (logs) das atividades

da solução de criptografia e visualizar, testar e modificar as configurações de rede;

8.12.12.29. O acesso a este ambiente de execução de procedimentos de identificação de problema e realização de tarefas administrativos deve ser controlado através de política gerenciada remotamente pelo componente de gerenciamento da solução;

8.12.12.30. Deve prover ferramenta presente na estação de trabalho que possibilite migrá-la para um servidor de gerenciamento diferente;

8.12.12.31. Deve permitir a gerência das seguintes soluções terceiras de criptografia:

- Microsoft bitlocker;
- Apple filevault.

8.12.12.32. As capacidades de gerência das soluções terceiras de criptografia devem incluir:

- Habilitar a criptografia;
- Exibir o estado da criptografia (ativado, desativado);
- Habilitar o aviso legal;
- Editar o intervalo de sincronia.

8.12.12.33. Deve permitir a visualização das estações de trabalho que tenham aplicação de política pendente a partir da console de administração centralizada;

8.12.12.34. Deve permitir a visualização do autor de determinada política a partir da console de administração centralizada;

8.12.12.35. Deve permitir a visualização de estações de trabalho que não possuam nenhuma política aplicada a partir da console de administração centralizada;

8.12.12.36. Deve permitir a adição de informações de contato a serem exibidas ao usuário final com texto customizável;

8.12.12.37. Deve permitir a exibição de aviso legal quando o agente de criptografia é instalado na estação de trabalho;

8.12.12.38. Deve permitir a exibição de aviso legal quando a estação é inicializada;

8.12.12.39. Deve permitir, em nível de política, a indicação de pastas a serem criptografadas;

8.12.12.40. Deve possibilitar que cada política tenha uma chave de criptografia única;

8.12.12.41. Deve permitir, em nível de política, a escolha da chave de criptografia a ser utilizada, entre as seguintes opções:

- Chave do usuário: somente o usuário tem acesso aos arquivos;
- Chave da empresa: qualquer usuário da empresa tem acesso aos arquivos;
- Chave da política: qualquer estação de trabalho que tenha aplicada a mesma política tem acesso aos arquivos.

8.12.12.42. Deve permitir a escolha dos diretórios a serem criptografados em dispositivos de armazenamento USB;

8.12.12.43. Deve possibilitar a desativação de dispositivos de gravação de mídias óticas;

8.12.12.44. Deve possibilitar a desativação de dispositivos de armazenamento USB;

8.12.12.45. Deve possibilitar o bloqueio da desinstalação do agente de criptografia por usuários que não sejam administradores da estação de trabalho;

8.12.12.46. Deve possibilitar o bloqueio da autenticação de usuários baseado no intervalo em que o dispositivo não tenha as políticas sincronizadas com o componente de administração centralizada;

8.12.12.47. Deve possibilitar o atraso, em intervalo personalizado de tempo, para uma nova tentativa de autenticação de usuários na ocorrência de um número personalizável de tentativas inválidas de autenticação;

8.12.12.48. Deve possibilitar apagar todos os dados do dispositivo na ocorrência de um número personalizável de tentativas inválidas de autenticação;

8.12.12.49. Deve possibilitar a instauração de política de gerenciamento de complexidade e intervalo de troca de senha com os seguintes critérios:

8.12.12.50. Definição do intervalo de dias em que o usuário será forçado a mudar sua senha;

8.12.12.51. Definição de número de senhas imediatamente anteriores que não poderão ser reutilizadas como nova senha;

8.12.12.52. Definição do número de caracteres iguais consecutivos que não poderão ser utilizados na nova senha;

8.12.12.53. Definição do comprimento de caracteres mínimo a ser utilizado na nova senha;

8.12.12.54. Definição do número de caracteres especiais, caracteres numéricos, caracteres em caixa alta e caracteres em caixa baixa que deverão ser utilizados para a nova senha;

8.12.12.55. Deve permitir a criação de múltiplos painéis (dashboards) personalizáveis, compostos por blocos de informações (widgets), visualizados através de gráficos ou tabelas quando integrado com o a console de gerenciamento;

8.12.12.56. Os blocos de informações pertencentes aos painéis personalizáveis devem permitir filtros personalizados para facilitar na visualização e gerenciamentos;

8.12.12.57. A seleção de uma informação específica dentro de um bloco de informações, através de um clique, deve redirecionar ao log detalhado que gerou aquela informação;

8.12.12.58. Deve possuir a funcionalidade de instalação remota do agente usando a mesma comunicação do Anti-virus;

8.12.12.59. Deve possuir uma ferramenta de recovery em caso de problema com o boot do Sistema Operacional.

8.12.13. Módulo de proteção para smartphones e tablets:

8.12.13.1. O módulo de proteção de dispositivos móveis deve possuir agente para os seguintes sistemas operacionais:

- IOS, Android e Windows phone.

8.12.13.2. As funcionalidades estarão disponíveis de acordo com cada plataforma;

8.12.13.3. Deve permitir o provisionamento de configurações de:

- Wi-fi, Exchange Activesync, vpn, proxy http global e certificados.

8.12.13.4. Deve possuir proteção de anti-malware;

8.12.13.5. Deve ser capaz de realizar escaneamento de malwares em tempo real, do cartão sd e após atualização de vacinas;

8.12.13.6. Deve possuir capacidade de detecção de spam proveniente de SMS;

8.12.13.7. Deve possuir funcionalidade de filtro de chamadas que possibilita a criação de lista de número bloqueados para recebimento de chamadas;

8.12.13.8. Deve possuir funcionalidade de filtro de chamadas que possibilita a criação de lista de número permitidos para efetuação de chamadas;

8.12.13.9. Deve possuir a possbilidade de criar uma loja de aplicativos;

8.12.13.10. Deve possuir funcionalidade de firewall para bloqueio de tráfego de entrada e saída, com possibilidades de enumeração de regras de exceção;

8.12.13.11. Deve permitir a proteção contra ameaças provenientes da web por meio de um sistema de reputação de segurança das URL's acessadas;

8.12.13.12. Deve permitir o controle de acesso a websites por meio de listas de bloqueio e aprovação;

8.12.13.13. Deve possuir a capacidade integração com Soluções Mobile de terceiros como Air Watch e Mobile Iron;

8.12.13.14. Deve permitir o bloqueio de aplicativos de acordo com sua faixa etária indicativa;

8.12.13.15. Deve possuir a funcionalidade de relatórios por plataforma;

8.12.13.16. Os relatórios deveram trazer informações sobre detecção de malware, acessos a sites maliciosos, inventario de aplicações, dispositivos que violaram a política;

8.12.13.17. A solução de segurança mobile deve possuir integração com o Samsung KNOX;

8.12.13.18. A solução de segurança *mobile* deverá enviar um convite para e-mail com informações para o usuário fazer a instalação do agente de segurança;

8.12.13.19. A solução de segurança *mobile* deverá possuir o aplicativo disponível nas lojas da *Apple* e *Google Play*;

8.12.13.20. Deve possuir integração com Microsoft *Active Directory*;

8.12.13.21. Os relatórios agendados devem ser pelo menos diário, semanal e mensal;

8.12.13.22. Controle da política de segurança de senhas, com critérios mínimos de:

- Padrão de senha;
- Uso obrigatório de senha;
- Tamanho mínimo;
- Tempo de expiração;
- Bloqueio automático da tela;
- Bloqueio por tentativas inválidas;
- Controle de acesso à seguinte lista funções e status de ativação de funções dos dispositivos móveis:

- Bluetooth;
- Descoberta de dispositivos *bluetooth*;
- Câmera;
- Cartões de memoria;
- *Wlan/wifi*;
- Aceitar TLS não confiável;
- Instalação de aplicativos;
- Sincronia automática enquanto em modo *roaming*;
- Dados de diagnostico;
- Forçar backups criptografados;
- *Itunes*;
- *Imessage*;
- Compra dentro de aplicativos;
- Remoção de aplicativos;
- Safari;
- Autopreenchimento;
- *Javascript*;
- *Popups*;
- Forçar aviso de fraude;
- Aceitar cookies;
- Captura de tela;
- Siri;
- Siri com tela bloqueada;
- Filtro de profanidade;
- Jogos multijogador;
- Discagem por voz;
- Youtube;
- Abertura de documentos de aplicativos gerenciados em aplicativos terceiros;
- Abertura de documentos de aplicativos terceiros em aplicativos gerenciados;
- GPS;
- Microsoft Activesync;
- MMS/SMS;
- Porta infravermelha;
- Porta serial;
- Alto-falante;
- Armazenamento USB;
- 3g;
- Modo de FABRICANTE;
- Ancoragem (tethering).

8.12.14. Módulo Gerenciamento Centralizado:

8.12.14.1. A solução de gerenciamento centralizado deve permitir a integração com a solução de segurança para proteção de estações de trabalho (desktops e notebooks) e prover visibilidade das soluções que possui integração;

8.12.14.2. Instalação do servidor na plataforma Windows 2008 Server ou superior, seja o servidor físico ou virtual;

8.12.14.3. Suportar base de dados Microsoft SQL;

8.12.14.4. Deve gerenciar logs das atividades e eventos gerados pela solução;

8.12.14.5. Deve possuir integração com Microsoft Active Directory;

8.12.14.6. Deve permitir níveis de administração por usuários ou grupos de usuários;

8.12.14.7. Deve permitir a constituição de políticas genéricas aplicáveis a grupos de máquinas, ou aplicáveis a grupos de usuários;

8.12.14.8. Deve disponibilizar sua interface através dos protocolos http e https;

8.12.14.9. Deve permitir a alteração das configurações das ferramentas ofertadas, de maneira remota;

8.12.14.10. Deve permitir diferentes níveis de administração, de maneira independente do login da rede;

8.12.14.11. Geração de relatórios e gráficos e parametrizáveis nos formatos html, pdf, xml e csv;

8.12.14.12. Deve gerar relatórios e gráficos pré-definidos nos formatos rtf, pdf, Activex e crystal report (*.rpt);

8.12.14.13. Deve permitir criação de modelos de relatórios customizados;

8.12.14.14. Deve permitir logon via single sign-on com os demais produtos da solução;

8.12.14.15. Deve permitir a atualização de todos os componentes de todos os módulos gerenciados;

8.12.14.16. Deve permitir a criação de planos de entrega das atualizações, com hora de início ou postergação da entrega após o download dos componentes;

8.12.14.17. Deve permitir o controle individual de cada componente a ser atualizado;

8.12.14.18. Deve permitir a definição de exceções por dias e horas para não realização de atualizações;

8.12.14.19. Deve permitir ter como fonte de atualização um compartilhamento de rede no formato UNC;

8.12.14.20. Deve gerar relatórios e gráficos com o detalhamento das versões dos produtos instalados;

8.12.14.21. Deve possuir o acompanhamento dos comandos administrativos em execução, tal como seu status de conclusão, alvo e usuário;

8.12.14.22. Deve permitir a configuração dos eventos administrativos ou de segurança que geram notificações, tal como o método de envio e o destinatário;

8.12.14.23. Os métodos de envio suportados devem incluir: e-mail, gravação de registros de eventos do Windows, SNMP e SYSlog;

8.12.14.24. Deve permitir a configuração do intervalo de comunicação com os módulos gerenciados;

8.12.14.25. Deve permitir a escolha do intervalo de tempo necessário para que um módulo seja considerado fora do ar (off-line);

8.12.14.26. Deve permitir o controle do intervalo de expiração de comandos administrativos;

8.12.14.27. Deve possuir a configuração do tempo de expiração da sessão dos usuários;

8.12.14.28. Deve permitir a configuração do número de tentativa inválidas de login para o bloqueio de usuários;

8.12.14.29. Deve permitir a configuração da duração do bloqueio;

8.12.14.30. Deve permitir pesquisas personalizadas para a consulta de eventos (logs) através de categorias

8.12.14.31. Deve permitir pesquisas personalizadas para a consulta de eventos (logs), através de critérios lógicos, com base em todos os campos pertencentes aos eventos consultados;

8.12.14.32. Deve permitir a configuração das informações que não são enviadas dos módulos à solução de gerenciamento centralizado;

8.12.14.33. Deve permitir a configuração da manutenção dos registros de eventos (logs), com base no intervalo de tempo que devem ser mantidos e no número máximo de registros, por tipo de evento;

8.12.14.34. Deve de permitir a criação de políticas de segurança personalizadas;

8.12.14.35. As políticas de segurança devem permitir a seleção dos alvos baseados nos seguintes critérios:

8.12.14.36. Nome parcial ou completo das estações de trabalho, permitindo a utilização de caractere coringa para identificação do nome parcial da máquina;

8.12.14.37. Range de endereços IPS;

8.12.14.38. Sistema operacional;

8.12.14.39. Agrupamento lógicos dos módulos;

8.12.14.40. As políticas de segurança devem permitir a combinação lógica dos critérios para identificação do(s) alvo(s) de cada política;

8.12.14.41. Deve permitir visualização de eventos de violação de segurança de todos os módulos gerenciados, agrupado por usuário numa linha de tempo, configurável;

8.12.14.42. Deve permitir a gerencia dos módulos baseados no modelo de nuvem (cloud), quando existentes;

8.12.14.43. Deve permitir a criação de múltiplos painéis (dashboards) personalizáveis, compostos por blocos de informações (widgets), visualizados através de gráficos ou tabelas;

8.12.14.44. Os blocos de informações pertencentes aos painéis personalizáveis devem permitir filtros personalizados para facilitar na visualização e gerenciamentos;

8.12.14.45. A seleção de uma informação específica dentro de um bloco de informações, através de um clique, deve redirecionar ao log detalhado que gerou aquela informação;

8.12.14.46. Deve possuir repositório central de identificadores de dados, que podem ser utilizados para a criação de políticas contra possíveis vazamentos de informações;

8.12.14.47. Deve permitir a investigação de incidentes de vazamento de informação através de um número identificador de incidentes.

8.13. **Expansão *Storage* EVA 4400:**

8.13.1. A contratada deverá fornecer os itens abaixo para expansão de 02 (dois) Storage HP 4400 EVA que encontrasse instalado na Prefeitura Municipal de Foz do Iguaçu e no Hospital regional de Foz do Iguaçu:

8.13.2. 2 (Dois) Enclosures compatíveis com HP 4400 EVA;

8.13.3. 24 (vinte e quatro) Discos rígidos 1TB FATA compatíveis com HP 4400 EVA;

8.13.4. A expansão deve adicionar no mínimo 12TB bruto ao Storage EVA 4400 instalado em cada localidade;

8.13.5. A expansão deverá vir acompanhada de todos os cabos, conectores, GBICs/SFPs, drivers, softwares, etc, necessários para acoplamento ao Storage como um item de expansão do mesmo;

8.13.6. A contratada deve realizar o planejamento e "site survey" detalhado, incluindo indicação das atualizações necessárias aos ambientes operacionais em produção, para que a solução seja suportada;

8.13.7. Instalação e configuração dos componentes da Solução proposta;

8.13.8. Testes e verificação do perfeito funcionamento da solução proposta.

8.14. **Consultoria Especializada Security N2 e N3:**

8.14.1. O serviço de consultoria especializada Security N2 e N3 deve fornecer 10 horas mensais, não cumulativas, de suporte técnico remoto via telefone e/ou E-mail com cobertura 8x5xNBD durante 12 meses para uso sob demanda do órgão PMFI;

8.14.2. O serviço deverá contemplar somente consultoria sobre assuntos e temas técnicos relacionados com os produtos/tecnologias de segurança contidos nesse edital;

8.14.3. O escopo do serviço de consultoria especializada Security N2 e N3 deve ser:

8.14.3.1. Orientações sobre uso, configuração e instalação dos produtos adquiridos, contando com acesso ao conhecimento privilegiado de recursos acerca de arquitetura tecnológica, viabilizando a definição de parâmetros objetivos para o dimensionamento da infraestrutura;

8.14.3.2. Questões sobre compatibilidade e interoperabilidade dos produtos adquiridos (hardware e software);

8.14.3.3. Orientação quanto às melhores práticas para implementação dos produtos adquiridos;

8.14.3.4. Análise técnica qualificada da compatibilidade e interoperabilidade dos produtos;

8.14.3.5. Aplicação de melhores práticas para implementação dos produtos adquiridos;

8.14.3.6. Estudo e reconfiguração do ambiente, quando esta demandar redimensionamento;

8.14.3.7. Estudo de revisão de arquitetura para melhoria de desempenho e disponibilidade;

8.14.3.8. Estudo e implementação de novas integrações ou ainda não previstas;

8.14.3.9. Indicação de modelos de uso e planejamento de capacidade;

8.14.3.10. Identificação de melhorias e respectivo tratamento (melhoria de parametrização);

8.14.3.11. Parametrização da solução, de acordo com as regras disponíveis na própria ferramenta e definidas pela Contratante;

8.14.3.12. Suporte Avançado técnico para estratégia e planejamento de migrações e adequações nos ambientes;

8.14.3.13. Planejamento de repasse de conhecimento e workshops de evolução das soluções.

8.14.4. A contratada deverá dispor de profissionais especializados e oficialmente certificados pelos respectivos fabricantes das soluções, para prestação do serviço de consultoria;

8.14.5. Os níveis de qualificação técnica e certificação oficial dos profissionais que irão prestar o serviço de consultoria deverão ser obrigatoriamente:

8.14.5.1. Firewall: Nível máximo Expert, não sendo aceitos níveis "associados" ou "Entry-Level";

8.14.5.2. E-mail Gateway: Nível Profissional ou Expert, não sendo aceitos níveis "associados" ou "Entry-Level".

8.14.5.3. Segurança Web: Nível Profissional ou Expert, não sendo aceitos níveis "associados" ou "Entry-Level".

8.15. **Consultoria Especializada Routing and Switching N2 e N3:**

8.15.1. O serviço de consultoria especializada Routing and Switching N2 e N3 deve fornecer 10 horas mensais, não cumulativas, de suporte técnico remoto via telefone e/ou E-mail com cobertura 8x5xNBD durante 12 meses para uso sob demanda do órgão PMFI

8.15.2. O serviço deverá contemplar somente consultoria sobre assuntos e temas técnicos relacionados com os produtos/tecnologias de segurança contidos nesse edital;

8.15.3. O escopo do serviço de consultoria especializada Routing and Switching N2 e N3 deve ser:

8.15.3.1. Orientações sobre uso, configuração e instalação dos produtos adquiridos, contando com acesso ao conhecimento privilegiado de recursos acerca de arquitetura tecnológica, viabilizando a definição de parâmetros objetivos para o dimensionamento da infraestrutura;

8.15.3.2. Questões sobre compatibilidade e interoperabilidade dos produtos adquiridos (hardware e software);

8.15.3.3. Orientação quanto às melhores práticas para implementação dos produtos adquiridos;

8.15.3.4. Análise técnica qualificada da compatibilidade e interoperabilidade dos produtos;

8.15.3.5. Aplicação de melhores práticas para implementação dos produtos adquiridos;

8.15.3.6. Estudo e reconfiguração do ambiente, quando esta demandar redimensionamento;

8.15.3.7. Estudo de revisão de arquitetura para melhoria de desempenho e disponibilidade;

8.15.3.8. Estudo e implementação de novas integrações ou ainda não previstas;

8.15.3.9. Indicação de modelos de uso e planejamento de capacidade;

8.15.3.10. Identificação de melhorias e respectivo tratamento (melhoria de parametrização);

8.15.3.11. Parametrização da solução, de acordo com as regras disponíveis na própria ferramenta e definidas pela Contratante;

8.15.3.12. Suporte Avançado técnico para estratégia e planejamento de migrações e adequações nos ambientes;

8.15.3.13. Planejamento de repasse de conhecimento e workshops de evolução das soluções.

8.15.4. A contratada deverá dispor de profissionais especializados e oficialmente certificados pelos respectivos fabricantes das soluções, para prestação do serviço de consultoria;

8.15.5. Os níveis de qualificação técnica e certificação oficial dos profissionais que irão prestar o serviço de consultoria deverão ser obrigatoriamente:

8.15.5.1. Routing and Switching: Nível máximo Expert, não sendo aceitos níveis "associados" ou "Entry-Level".

8.16. **Consultoria Especializada *VMWARE*:**

8.16.1. O serviço de consultoria especializada VMware consiste em prestar consultoria e orientação técnica para melhoria no ambiente, continuidade do processo de implantação e integração, desenvolvimento de competências técnicas, e o seu escopo compreende:

8.16.1.1. A contratada deve realizar o planejamento e "site survey" detalhado, incluindo indicação das atualizações e adequações necessárias ao ambiente operacional em produção, para que a solução seja suportada;

8.16.1.2. Orientações sobre uso, configuração e instalação dos produtos Vmware que a contratante possui em produção no seu ambiente, contando com acesso ao conhecimento privilegiado acerca de arquitetura tecnológica, viabilizando a definição de parâmetros objetivos para o dimensionamento da infraestrutura;

8.16.1.3. Questões sobre compatibilidade e interoperabilidade dos produtos VMware;

8.16.1.4. Orientação quanto às melhores práticas para implementação dos produtos de software VMware para os cenários de falha;

8.16.1.5. Apoio e/ou atuação direta na execução de procedimentos de atualização para novas versões dos produtos de softwares instalados;

8.16.1.6. Análise técnica qualificada da compatibilidade e interoperabilidade dos produtos;

8.16.1.7. Aplicação de melhores práticas para implementação dos produtos de software VMware;

8.16.1.8. Estudo e reconfiguração do ambiente, quando esta demandar redimensionamento;

8.16.1.9. Estudo de melhoria do ambiente atual (infraestrutura) no qual esteja inserida qualquer ferramenta, individualmente ou com as integrações correlatas;

8.16.1.10. Estudo de revisão de arquitetura para melhoria de desempenho e disponibilidade;

8.16.1.11. Indicação de modelos de uso e planejamento de capacidade;

8.16.1.12. Parametrização da solução, de acordo com as regras disponíveis na própria ferramenta e definidas pela Contratante;

8.16.1.13. Apoio para execução de procedimentos de atualização para novas versões dos produtos de softwares instalados;

8.16.1.14. Apoio à elaboração e adequação de relatórios executivos, gerenciais e operacionais;

8.16.1.15. Suporte Avançado técnico para estratégia e planejamento de migrações e adequações nos ambientes;

8.16.1.16. Planejamento de repasse de conhecimento e workshops de evolução das soluções.

8.17. **Treinamentos Oficiais:**

8.17.1. ***Firewall*:**

8.17.1.1. Treinamento presencial oficial para 04 (quatro) servidores da PMFI;

8.17.1.2. Deverá ser entregue em formato de Voucher com validade para pelo menos 1 ano;

8.17.1.3. Os treinamentos deverão capacitar o técnico/analista a instalar, configurar e gerenciar os equipamentos firewall, bem como a habilitar o analista/técnico a gerenciar ameaças cibernéticas "cyberthreads", além de depurar e solucionar problemas nos equipamentos;

8.17.1.4. Deve abordar pelo menos os seguintes tópicos:

- Gerenciamento e Relatórios;
- VPNs;
- Anti-Malware;
- Vulnerabilidades;
- Filtragem de URLs;
- Segurança e Politicas NAT Basico e Avançado;
- Politicas Avançadas de Encaminhamento de Pacotes;
- OSPF;
- Zonas de Segurança;
- Encaminhamento de Logs;
- SNMP;
- Assinaturas de ameaças;
- Troubleshoting VPN;
- TroubleShooting Layer 3;
- TroubleShooting Performance.

8.17.1.5. O Treinamento completo deverá estar disponível no calendário do fabricante pelo menos uma vez a cada trimestre;

8.17.1.6. O curso deverá possuir carga horária com no mínimo 20 horas e ser prestado em dias úteis entre 8:00 e 18:00;

8.17.1.7. A contratada deverá fornecer todo material didático necessário para o treinamento;

8.17.1.8. Uma vez solicitado o desconto do Voucher a contratada deverá se responsabilizar por todo o tramite junto ao fabricante, disponibilização do número de vagas solicitado e caso o treinamento não seja realizado em Foz do Iguaçu, a empresa proponente deverá providenciar o transporte, hospedagem, alimentação e translado para todos os participantes do curso arcando com suas despesas;

8.17.1.9. O curso deve ser ministrado em língua portuguesa por profissional certificado junto ao respectivo fabricante da solução ofertada;

8.17.1.10. As datas serão definidas em comum acordo entre a contratada e a PMFI.

8.17.2. ***Switches*/*Roteadores*:**

8.17.2.1. Treinamento presencial oficial para 04(quatro) servidores da PMFI. Deverá ser entregue em formato de Voucher com validade de pelo menos um ano;

8.17.2.2. Os treinamentos deverão capacitar o técnico/analista a instalar, configurar e gerenciar os equipamentos, além de depurar e solucionar problemas nos equipamentos. Devendo abordar pelo menos os seguintes tópicos:

- Introdução aos produtos de networking e resumo de comandos CLI;
- Interfaces (Physical, Port Channel, VLANs);
- Introdução sobre o protocolo *spanning tree* (STP, RSTP, PVST e MSTP);
- Introdução, Configuração e Utilização de ACL's (Access Control Lists) e PBRs (Police Base Routing);
- Configuração e Troubleshooting do protocolo VRRP;
- Introdução e métodos de configurações sobre IPv6;
- Conceitos de Roteamento;
- Introdução, Configuração básica e troubleshooting de roteamento estático;
- Introdução, Configuração básica e troubleshooting dos protocolos de OSPF e RIP;
- Introdução, Configuração básica e troubleshooting do protocolo de roteamento OSPFv3, RIP e BGP;
- Introdução e configuração de *stacking*.

8.17.2.3. O Treinamento completo deverá estar disponível no calendário do fabricante pelo menos uma vez a cada trimestre;.

8.17.2.4. O curso deverá possuir carga horária com no mínimo 20 horas e ser prestado em dias úteis entre 8:00 e 18:00;

8.17.2.5. A contratada deverá fornecer todo material didático necessário para o treinamento;

8.17.2.6. Uma vez solicitado o desconto do Voucher a contratada deverá se responsabilizar por todo o tramite junto ao fabricante, disponibilização do número de vagas solicitado e caso o treinamento não seja realizado em Foz do Iguaçu, a empresa proponente deverá providenciar o transporte, hospedagem, alimentação e translado para todos os participantes do curso arcando com suas despesas;

8.17.2.7. O curso deve ser ministrado em língua portuguesa por profissional certificado junto ao respectivo fabricante da solução ofertada;

8.17.2.8. As datas serão definidas em comum acordo entre a contratada e a PMFI.

8.17.3. **Solução de Segurança *Web*:**

8.17.3.1. Treinamento presencial oficial para 04(quatro) servidores da PMFI. Deverá ser entregue em formato de Voucher com validade de pelo menos um ano;

8.17.3.2. Os treinamentos deverão capacitar o técnico/analista a instalar, configurar e gerenciar os equipamentos, além de depurar e solucionar problemas nos equipamentos. Devem abordar pelo menos os seguintes tópicos:

- Conceitos de design e configuração de sistemas de caching e proxy (explicit proxy, transparent proxy, auto-discovery), nomenclaturas, protocolos, autenticaçãobem como a integração com outros serviços de rede, notadamente DNS, Windows AD e serviços de backup;
- Configuração de proxy HTTP, HTTPS, SOCKS e FTP;
- Conceitos de QoS e configuração dePBR, controle de banda por aplicação, identificação de aplicações, bloqueio, uso de políticas por tempo;
- Configuração de filtros de URL;
- Configuração de SSL, portais de autenticação;
- Uso de antivírus e identificação avançada de malwares;
- Geração de relatórios, incluindo criação de templates;
- Monitoramento;
- Introdução, configuração e utilização de políticas incluindo filtragem e controle de aplicações e micro aplicações por grupo de usuários, horário, etc.;

8.17.3.3. O Treinamento completo deverá estar disponível no calendário do fabricante pelo menos uma vez a cada trimestre;

8.17.3.4. O curso deverá possuir carga horária com no mínimo 20 horas e ser prestado em dias úteis entre 8:00 e 18:00;

8.17.3.5. A contratada deverá fornecer todo material didático necessário para o treinamento;

8.17.3.6. Uma vez solicitado o desconto do Voucher a contratada deverá se responsabilizar por todo o tramite junto ao fabricante, disponibilização do número de vagas solicitado e caso o treinamento não seja realizado em Foz do Iguaçu, a empresa proponente deverá providenciar o transporte, hospedagem, alimentação e translado para todos os participantes do curso arcando com suas despesas;

8.17.3.7. O curso deve ser ministrado em língua portuguesa por profissional certificado junto ao respectivo fabricante da solução ofertada;

8.17.3.8. As datas serão definidas em comum acordo entre a contratada e a PMFI.

8.17.4. **Solução de *E-mail Gateway*:**

8.17.4.1. Treinamento presencial oficial para 04 (quatro) servidores da PMFI. Deverá ser entregue em formato de Voucher com validade de pelo menos um ano;

8.17.4.2. Os treinamentos deverão capacitar o técnico/analista a instalar, configurar e gerenciar os equipamentos, além de depurar e solucionar problemas nos equipamentos. Devem abordar pelo menos os seguintes tópicos:

- Conceitos de design e configuração de sistemas email, incluindo blacklists, whitelists, spam blocking, gray email detection, anti-spoofing bem como a integração com outros serviços de rede, notadamente DNS, Windows AD e serviços de backup;
- Conceitos de QoS e configuração aplicados ao gerenciamento de filas e recepção e transmissão de e-mails, redundância;
- Configuração de criptografia e autenticação;
- Uso de antivírus e identificação avançada de malwares;
- Geração de relatórios, incluindo criação de templates;
- Monitoramento;
- Introdução, configuração e utilização de políticas incluindo filtragem e controle de aplicações e micro aplicações por grupo de usuários, horário, etc..

8.17.4.3. O Treinamento completo deverá estar disponível no calendário do fabricante pelo menos uma vez a cada trimestre;

8.17.4.4. O curso deverá possuir carga horária com no mínimo 20 horas e ser prestado em dias úteis entre 8:00 e 18:00;

8.17.4.5. A contratada deverá fornecer todo material didático necessário para o treinamento;

8.17.4.6. Uma vez solicitado o desconto do Voucher a contratada deverá se responsabilizar por todo o tramite junto ao fabricante, disponibilização do número de vagas solicitado e caso o treinamento não seja realizado em Foz do Iguaçu, a empresa proponente deverá providenciar o transporte, hospedagem, alimentação e translado para todos os participantes do curso arcando com suas despesas;

8.17.4.7. O curso deve ser ministrado em língua portuguesa por profissional certificado junto ao respectivo fabricante da solução ofertada;

8.17.4.8. As datas serão definidas em comum acordo entre a contratada e a PMFI.

9. OBRIGAÇÕES DA CONTRATADA

9.1. Prestar os serviços, entregar e instalar os equipamentos que compõem a solução de segurança e conectividade, objeto deste Termo de Referência, de acordo com as especificações e quantidades descritas;

9.2. A empresa deverá possuir equipe técnica de pessoal, própria, para execução do contrato;

9.3. Responder, em relação aos seus empregados, por todas as despesas decorrentes dos serviços, tais como: salários, seguros de acidentes, tributos, indenizações, vales refeição, vale-transporte e outras que porventura venham a ser regulada em acordo coletivo;

9.4. A Prefeitura Municipal de Foz do Iguaçu não se responsabilizará por qualquer despesa de responsabilidade do fornecedor ou correspondente aos técnicos alocados, como transporte, alimentação, salários, seguros de vida, etc.;

9.5. Executar diretamente o contrato, sem a transferência de responsabilidades ou subcontratações não autorizadas pela Prefeitura Municipal de Foz do Iguaçu;

9.6. Selecionar e treinar os empregados que irão prestar os serviços, tendo funções profissionais legalmente registradas em suas carteiras de trabalho;

9.7. Responder pelos danos causados diretamente a Prefeitura Municipal de Foz do Iguaçu ou a terceiros, decorrentes de sua culpa ou dolo;

9.8. Manter, os seus empregados uniformizados e identificados por crachá, quando em trabalho, devendo substituir imediatamente qualquer um deles que seja considerado inconveniente à boa ordem e às normas disciplinares da Prefeitura Municipal de Foz do Iguaçu;

9.9. Respeitar as normas e procedimentos de controle e acesso às dependências da Prefeitura Municipal de Foz do Iguaçu;

9.10. Arcar com despesas decorrentes de qualquer infração, seja qual for, desde que praticada por seus empregados, quando relacionados com a execução dos serviços;

9.11. Comunicar por escrito, a Prefeitura Municipal de Foz do Iguaçu, qualquer anormalidade verificada na execução dos serviços, relatando-as no Livro de Ocorrências, com os danos e circunstâncias julgados necessários ao relato e esclarecimento dos fatos;

9.12. Observar o horário de trabalho estabelecido pela Prefeitura Municipal de Foz do Iguaçu, em conformidade com as leis trabalhistas;

9.13. Manter, durante a execução do contrato as condições que ensejaram a contratação;

9.14. Informar ao Ministério Público a ocorrência de qualquer irregularidade ocorrida com os técnicos alocados;

9.15. Emitir e enviar, à Prefeitura Municipal de Foz do Iguaçu, notas fiscais de serviços (NFS-e) ou de aquisição de equipamentos (NF-e) de acordo com o cronograma de pagamentos pré-estabelecido em até 48 (quarenta e oito horas) após a entrega dos mesmos e aceite da PMFI/SMTI;

9.16. No valor da proposta deverão estar incluídos todos os encargos sociais, impostos, tributos, taxas, etc., inclusive aqueles que deverão ser recolhidos aos cofres do município.

10. DAS OBRIGAÇÕES DO CONTRATANTE

10.1. Efetuar o pagamento devido pela prestação dos serviços de implantação da solução pretendida, bem como pelo fornecimento e instalação dos equipamentos, desde que cumpridas todas as formalidades e exigências do contrato;

10.2. Sendo necessário, permitir o livre acesso dos empregados da licitante vencedora as dependências dos órgãos que compõem a administração pública do Governo Municipal, para execução dos serviços ora contratados, desde que devidamente identificados;

10.3. Prestar as informações e os esclarecimentos que venham a ser solicitado pelos empregados da licitante vencedora;

10.4. Comunicar a licitante vencedora, quaisquer irregularidades ocorridas, consideradas de natureza grave;

10.5. Solicitar, quando necessário, treinamentos ou substituições dos técnicos alocados;

10.6. Exercer a gestão, fiscalização, orientação e distribuição dos serviços, através da PMFI/SMTI, acompanhando a execução do contrato através de gestor e fiscal, devidamente investido;

10.7. Atestar as faturas correspondentes, pela SMTI.

11. DA GESTÃO E FISCALIZAÇÃO DO CONTRATO

11.1. Ficará a cargo da equipe técnica da SMTI - Secretaria Municipal de Tecnologia da Informação, a gestão, o acompanhamento e a fiscalização do contrato oriundo desta licitação, bem como da execução dos serviços e instalação dos equipamentos, designando para tanto os servidores, abaixo identificados, como:

11.1.1. **GESTOR do contrato:**

- **Nome:** Evandro ferreira;
- **Cargo/Função**: Secretário Municipal de Tecnologia da Informação.

11.1.2. **FISCAL do contrato:**

- **Nome:** Sandro Lopes Ebbing;

- **Cargo/Função:** Diretor de Infraestrutura e Segurança da Informação.

12. DO PREÇO E CONDIÇÕES DE PAGAMENTO

12.1. O valor máximo global admitido à ser pago pela CONTRATANTE à CONTRATADA, pela prestação dos serviços de fornecimento e implantação de solução para segurança e conectividade das áreas de Tecnologia da Informação (*hardwares* - equipamentos e *softwares* - sistemas) da Prefeitura Municipal de Foz do Iguaçu, incluindo-se o fornecimento de equipamentos e sistemas necessários para a ampliação e/ou a substituição de ativos de rede, *internet*, *firewall*, *switches* e roteadores, bem como *softwares* e demais sistemas necessários será de **R$2.203.362,15 (Dois milhões, duzentos e três mil, trezentos e sessenta e dois reais, e quinze centavos)**.

12.2. **Cronograma de pagamento:**

CRONOGRAMA DE PAGAMENTO				
ITEM	**TIPO**	**DESCRIÇÃO**	**VALOR**	**DATA**
1	Hardware	Firewall de Nova Geração – Firewall NGFW	R$ 308.647,16	+ 30 dias da assinatura do contrato
2	Software	Solução de Gerência e Relatórios para o Firewall NGFW	R$ 14.482,52	+ 30 dias da instalação
3	Hardware	Switches tipo 1 (agregador)	R$ 48.595,95	+ 30 dias da instalação
4	Hardware	Switches tipo 2 (core)	R$ 236.866,88	+ 30 dias da instalação
5	Hardware	Solução de Email Gateway (appliance físico)	R$ 266.169,79	+ 30 dias da instalação
6	Hardware	Solução de Segurança Web (appliance físico)	R$ 460.717,22	+ 30 dias da instalação
7	Hardware	Roteador de Borda Internet Multi-Serviço	R$ 257.306,52	+ 30 dias da instalação
8	Software	Solução de Endpoint Security	R$ 257.694,64	+ 30 dias da instalação
9	Hardware	Expansão Storage EVA 4400	R$ 93.817,59	+ 30 dias da instalação
10	Serviço	Consultoria Especializada Security N2 e N3	R$ 45.454,97	+ 30 dias da conclusão
11	Serviço	Consultoria Especializada Routing and Switching N2 e N3	R$ 51.245,67	+ 30 dias da conclusão
12	Serviço	Consultoria Especializada VMWARE	R$ 22.961,70	+ 30 dias da conclusão
13	Serviço	Treinamentos Oficiais – Categorias (4 alunos por categoria)	R$ 139.401,53	+ 30 dias da conclusão
TOTAL ==>>			**R$ 2.203.362,15**	

13. DA VIGÊNCIA DO CONTRATO

13.1. O Contrato decorrente desta licitação terá um prazo de duração de 12 (doze) meses podendo ser prorrogado de acordo com a Lei 8.666/1993.

14. DAS GARANTIAS CONTRATUAIS

14.1. Pelo atraso injustificado na execução do contrato sujeitará a CONTRATADA à multa de mora, na forma prevista no instrumento convocatório ou no contrato de acordo com o art. 86 da Lei 8.666/93;

14.2. Pela inexecução total ou parcial do contrato o município poderá, garantida a prévia defesa, aplicar a CONTRATADA as sanções previstas nos Artigos 87 e 88 da Lei 8.666/93.

15. DAS CONDIÇÕES PARA HABILITAÇÃO TÉCNICA DAS LICITANTES[2]

15.1. Realização de visita técnica, pela licitante, com vistas a conhecer os ambientes da área de Tecnologia da Informação da Prefeitura Municipal de Foz do Iguaçu sua estrutura (equipamentos e serviços em operação), versão de *hardwares* e *softwares*, condições e funcionalidades, bem como obter as informações necessárias a execução dos serviços de fornecimento e implantação de solução para segurança e conectividade da área de Tecnologia da Informação (*hardwares* - equipamentos e *softwares* - sistemas) da Prefeitura Municipal de Foz do Iguaçu, e dirimir as dúvidas, a fim de que a licitante possa participar do certame, com a certeza de que atende plenamente todas as necessidades e objetivos do Município na implementação da solução pretendida;

15.1.1. As visitas técnicas deverão ser previamente agendas com a Srª. Ricarda Agnes Castagnaro da Silva Kovacs, via telefone: (45) 2105-1007 ou via e-mail: smtirecepcao@pmfi.pr.gov.br, de segunda à sexta-feira durante o horário das 08 às 12 horas e das 13hs30min. às 17hs30min.;

15.1.2. **A visita técnica é facultativa.**

15.2. A licitante deverá comprovar a sua qualificação e experiência para execução dos serviços descritos neste Termo de Referência, objeto desta licitação, com acervo seu, em características e quantitativos semelhantes aos especificados no edital, através da apresentação de, no mínimo, 01 (um) atestado de capacidade técnica, fornecido por pessoa jurídica de direito público ou privado, que deverá ser compatível, no mínimo, com o objeto desta licitação, ou seja, comprovando a experiência em: prestação dos serviços de fornecimento e implantação de solução para segurança e conectividade da área de Tecnologia da Informação (*hardwares* - equipamentos e *softwares* - sistemas). O atestado deverá conter, no mínimo, as seguintes informações:

- O contratante com o seu endereço e CNPJ;
- A descrição do objeto da contratação;
- Especificação;
- Período de realização dos serviços;
- Manifestação expressa do Contratante de que a Proponente "atende/eu satisfatoriamente ao contratado"* ou manifestação do grau de satisfação do cliente (ex: bom, ótimo ou excelente)*, em relação aos serviços prestados.

15.2.1. Não serão considerados os Atestados que contenham ressalvas;

[2] **Constituem requisitos da habilitação, os itens 15.2 a 15.4, os demais itens deverão ser apresentados na assinatura do Contrato.**

15.2.2. Poderá ser realizada DILIGÊNCIA para comprovar a autenticidade do(s) Atestado(s) de Capacidade Técnica.

15.3. A licitante deverá comprovar a sua qualificação e experiência para execução dos serviços descritos neste Termo de Referência, objeto desta licitação, com acervo seu, em características e quantitativos semelhantes aos especificados no edital, através da apresentação de, no mínimo, 01 (um) atestado de capacidade técnica, fornecido por pessoa jurídica de direito público ou privado, que deverá ser compatível, no mínimo, com o objeto desta licitação, ou seja, comprovando a experiência em: prestação dos serviços de fornecimento de solução de backup com Serviços de Instalação, Migração de Ambiente, Ativação e Transferência de tecnologia. O atestado deverá conter, no mínimo, as seguintes informações:

- O contratante com o seu endereço e CNPJ;
- A descrição do objeto da contratação;
- Especificação;
- Período de realização dos serviços;
- Manifestação expressa do Contratante de que a Proponente "atende/eu satisfatoriamente ao contratado"* ou manifestação do grau de satisfação do cliente (ex: bom, ótimo ou excelente)*, em relação aos serviços prestados.

15.3.1. Não serão considerados os Atestados que contenham ressalvas;

15.3.2. Poderá ser realizada DILIGÊNCIA para comprovar a autenticidade do(s) Atestado(s) de Capacidade Técnica.

15.4. A licitante deverá comprovar a sua qualificação e experiência para execução dos serviços descritos neste Termo de Referência, objeto desta licitação, com acervo seu, em características e quantitativos semelhantes aos especificados no edital, através da apresentação de, no mínimo, 01 (um) atestado de capacidade técnica, fornecido por pessoa jurídica de direito público ou privado, que deverá ser compatível, no mínimo, com o objeto desta licitação, ou seja, comprovando a experiência em: prestação dos serviços de fornecimento de Solução de Virtualização com Serviços de Instalação, Migração de Ambiente, Ativação e Transferência de tecnologia. O atestado deverá conter, no mínimo, as seguintes informações:

- O contratante com o seu endereço e CNPJ;
- A descrição do objeto da contratação;
- Especificação;
- Período de realização dos serviços;
- Manifestação expressa do Contratante de que a Proponente "atende/eu satisfatoriamente ao contratado"* ou manifestação do grau de satisfação do cliente (ex: bom, ótimo ou excelente)*, em relação aos serviços prestados.

15.4.1. Não serão considerados os Atestados que contenham ressalvas;

15.4.2. Poderá ser realizada DILIGÊNCIA para comprovar a autenticidade do(s) Atestado(s) de Capacidade Técnica.

15.5. A Contratada deverá fornecer o Projeto de Implementação, onde deverão constar procedimentos de validação para cada fase de implantação, seguindo as melhores práticas do fabricante e recomendando ações para correção de possíveis inconformidades, bem como Cronograma detalhado de Atividades. O cronograma detalhado deverá ser aprovado em comum acordo entre a LICITADA e a LICITANTE;

15.6. Para a execução dos serviços da solução proposta, a licitante deverá indicar na proposta a composição da equipe de especialistas, empregados ou consultores da contratada em sua proposta;

15.7. Pelo menos 02 (dois) técnicos, que deverão ser os responsáveis técnicos pelo atendimento a Contratante, deverá ter vínculo empregatício comprovado[3] através de **Registro em Carteira de Trabalho**, apresentando a original e cópia autenticada para ser entregue a Contratante; ou que conste no **Contrato Social** da Empresa, devendo neste caso ser fornecido uma cópia autenticada do mesmo; ou Ficha de empregado ou **contrato de trabalho**, sendo possível a contratação de profissional autônomo que preencha os requisitos e se responsabilize tecnicamente pela execução dos serviços;

15.8. Para a Solução de Firewall NGFW, a licitante deverá ter em seu quadro de funcionários CLT um analista de segurança da informação especializado e com certificação oficial válida de nível máximo de segurança da fabricante;

15.9. Para a Solução de Router de Borda Internet e Switches Core, a licitante deverá ter em seu quadro de funcionários CLT um analista de conectividade (Routing and Switching) especializado e com certificação oficial válida de nível máximo nas tecnologias roteadores e switches;

15.10. A licitante deverá comprovar ser parceira oficial autorizada da fabricante dos equipamentos e softwares relacionados a Solução Firewall NGFW, Solução de Segurança de E-mail e Solução de Segurança WEB, especificados neste Termo de Referência, apresentando certificado de nível máximo de parceria no Brasil, emitido pela fabricante ou ainda através do sítio da fabricante na internet;

15.11. A licitante deverá comprovar ser parceira autorizada da fabricante dos softwares relacionados ao Módulo de Proteção Anti-Malware, deste Termo de Referência, apresentando certificado, emitido pela fabricante ou ainda através do sítio da fabricante na internet;

15.12. A Empresa licitante deverá comprovar ser parceiro autorizado da Fabricante da VMWARE, através de Certificado emitido pelo Fabricante ou ainda através do Sítio na Internet do Fabricante do Software;

15.13. A Empresa licitante deverá comprovar, através de Certificado emitido pela VMWARE ou ainda através do Sítio na Internet do Fabricante de que está capacitada e habilitada a prestar serviços de virtualização nas seguintes áreas: Virtualização de Infraestrutura e Continuidade de Negócios.

15.14. A licitante deverá apresentar declaração de que os serviços serão prestados por técnicos habilitados, comprovando dispor por ocasião da convocação para assinatura do contrato, de um quadro de técnicos certificados, que, obrigatoriamente deverá abranger, de forma coletiva, a certificação abaixo:

- Certificação para solução, onde o fabricante reconhece que os profissionais com tal certificação, emitida pela própria, passou por todos os treinamentos adequados para realizar tarefas dentro dos padrões de qualidade e melhores práticas determinadas pelo fabricante e o capacita aprestar os serviços de configuração, design, gerenciamento, reconhecimento rápido de falhas e adequação da ferramenta de virtualização adquirida. Isso garantirá que o ambiente seja adequado corretamente de acordo as recomendações técnicas do fabricante;

[3] Para comprovação do vínculo, é aceito o Contrato de Prestação de Serviços, além dos mencionados no item 15.7.

- VCP-CMA Vmware Certified Professional Cloud Management & Automation - O fabricante reconhece que os profissionais com tal certificação, emitida pela própria, passou por todos os treinamentos adequados para realizar tarefas dentro dos padrões de qualidade e melhores práticas determinadas pelo fabricante e o capacita a prestar os serviços de configuração, design, gerenciamento, reconhecimento rápido de falhas e adequação da ferramenta de virtualização adquirida. Isso garantirá que o ambiente seja adequado corretamente de acordo as recomendações técnicas do fabricante;
- VCP-DCV Vmware Certified Professional Data Center Virtualization - O fabricante reconhece que os profissionais com tal certificação, emitida pela própria, passou por todos os treinamentos adequados para realizar tarefas dentro dos padrões de qualidade e melhores práticas determinadas pelo fabricante e o capacita a prestar os serviços de configuração, design, gerenciamento, reconhecimento rápido de falhas e adequação da ferramenta de virtualização adquirida. Isso garantirá que o ambiente seja adequado corretamente de acordo as recomendações técnicas do fabricante;
- VCP-NV Vmware Certified Professional Network Virtualization- O fabricante reconhece que os profissionais com tal certificação, emitida pela própria, passou por todos os treinamentos adequados para realizar tarefas dentro dos padrões de qualidade e melhores práticas determinadas pelo fabricante e o capacita a prestar os serviços de configuração, design, gerenciamento, reconhecimento rápido de falhas e adequação da ferramenta de virtualização adquirida. Isso garantirá que o ambiente seja adequado corretamente de acordo as recomendações técnicas do fabricante;
- VTSP Virtual Technical Solutions Professional - O fabricante reconhece que os profissionais com tal certificação, emitida pela própria, passou por todos os treinamentos adequados para realizar tarefas dentro dos padrões de qualidade e melhores práticas determinadas pelo fabricante e o capacita a prestar os serviços de configuração, design, gerenciamento, reconhecimento rápido de falhas e adequação da ferramenta de virtualização adquirida. Isso garantirá que o ambiente seja adequado corretamente de acordo as recomendações técnicas do fabricante.

16. CONDIÇÕES PARA PARTICIPAÇÃO

16.1. Poderão participar da presente licitação as empresas devidamente habilitadas a executar o objeto desta licitação, na forma estabelecida na Lei 8.666/93, Lei 10.520/02 e Lei 123/2006;

16.2. Só poderão participar desta licitação empresas cujo objeto social ou ramo de atuação sejam pertinentes ao objeto desta licitação e desde que atendam a todos os requisitos estabelecidos nesta Concorrência Pública, seus anexos e legislação em vigor;

16.3. Não poderão participar desta licitação as empresas interessadas que se encontrem sob falência, recuperação judicial, concurso de credores, dissolução e liquidação;

16.4. Não será admitida a subcontratação total dos serviços licitados. Somente será admitida subcontratação parcial mediante prévia e expressa autorização do Prefeito Municipal;

17. DAS TÉCNICAS NECESSÁRIAS

17.1. Concorrência Pública, do Tipo Menor Preço Global, de acordo com Lei 8.666/93.

Foz do Iguaçu, 10 de julho de 2018.

Elaborado por: De Acordo:

Sandro Lopes Ebbing
Diretor de Infraestrutura e Segurança da Informação
PMFI - Portaria 63.392

Evandro ferreira
Secretário Mun. de Tecnologia da Informação
PMFI - Portaria 63.393

ANEXO III
DAS EXIGÊNCIAS DA PROPOSTA COMERCIAL E DA HABILITAÇÃO

1. DAS EXIGÊNCIAS DA PROPOSTA COMERCIAL

1.1. O encaminhamento de proposta para o sistema eletrônico pressupõe o pleno conhecimento e atendimento às exigências de habilitação previstas no Edital. O Licitante será responsável por todas as transações que forem efetuadas em seu nome no sistema eletrônico, assumindo como firmes e verdadeiras suas propostas e lances.

1.2. A proposta de preços inicial deverá ser digitalizada, através do site **www.licitacoes-e.com.br**, para análise e terá que:

I - **Preço global**, em moeda brasileira corrente.
II - Prazo de validade da proposta: 60 dias, a não especificação significa que a licitante concorda com os termos do edital;
III - Prazo de Pagamento: conforme cronograma de pagamento especificado no Anexo I – Termo de Referência;
VI - Prazo de prestação dos serviços: 12 (doze) meses.

1.3. É vedada a identificação do licitante antes do término da fase competitiva.

1.4. Será desclassificada a proposta que estiver elaborada em desacordo com os termos deste edital, que se oponha a qualquer dispositivo legal vigente ou que contenha preços excessivos ou manifestamente inexequíveis, preços simbólicos ou irrisórios.

1.5. Considerar-se-á inexequível a proposta que não venha a ter demonstrada sua viabilidade por meio de documentação que comprove que os custos envolvidos na contratação são coerentes com os de mercado do objeto deste Pregão.

1.6. Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderá ser efetuada diligência, na forma do § 3º do art. 43 da Lei nº 8.666/93, para efeito de comprovação de sua exequibilidade, podendo-se adotar, dentre outros, questionamentos junto à proponente (arrematante) para a apresentação de justificativas e comprovações em relação aos custos com indícios de inexequibilidade;

1.7. Não será aceita cobrança posterior de qualquer imposto, tributo ou assemelhado adicional, salvo se alterado ou criado após a data de abertura desta licitação e que venha expressamente a incidir sobre o objeto desta licitação, na forma da Lei.

1.8. Os tributos, emolumentos, contribuições sociais, fiscais e parafiscais que sejam devidos em decorrência direta ou indireta do objeto da licitação, serão de exclusiva responsabilidade do contribuinte, assim definido na Norma Tributária.

1.9. O licitante declara haver levado em conta, na apresentação de sua proposta, os custos, emolumentos, encargos, inclusive sociais, contribuições fiscais e parafiscais, bem como os tributos incidentes, não cabendo quaisquer reivindicações devidas a erros nessa avaliação.

1.10. A microempresa ou empresa de pequeno porte optante pelo Simples Nacional, que, por ventura venha a ser contratado, não poderá beneficiar-se da condição de optante e estará sujeito à retenção na fonte de tributos e contribuições sociais, na forma da legislação em vigor, em decorrência da sua exclusão obrigatória do Simples Nacional a contar do mês seguinte ao da contratação em consequência do que dispõem o art. 17, da Lei Complementar nº 123, de 14 de dezembro de 2006 e alterações.

2. DA HABILITAÇÃO

2.1. A licitante com a proposta classificada em primeiro lugar, deverá encaminhar a seguinte documentação:

2.1.1 Registro comercial, no caso de empresa individual;

2.1.2 Ato constitutivo, estatuto ou **contrato social +** alterações (ou somente consolidação) em vigor, devidamente registrado, em se tratando de sociedade comercial, e, no caso de sociedade por ações, acompanhado, de documentos de eleição de seus administradores; apresentado em uma das formas a seguir:

2.1.2.1 Contrato social, *se não houver alterações;*
2.1.2.2 Contrato social *e alterações posteriores, ou*
2.1.2.3 Contrato consolidado.[4]

2.1.3 Inscrição do ato constitutivo, no caso de sociedades civis, acompanhada de prova da diretoria em exercício;

2.1.4 Declaração conjunta que versa sobre Recebimento do Edital, Superveniência de fatos impeditivos da habilitação, Proibição do Trabalho de Menores e de Relação de emprego com servidores; conforme **modelo II**;

2.1.5 Declaração de Elaboração Independente de Proposta, conforme IN nº. 02 SLTI/MPOG, de 16 de setembro de 2009, de acordo com o **modelo III**.

2.1.6 Prova de inscrição no Cadastro Nacional da Pessoa Jurídica (CNPJ);

[4] Uma alteração contratual consolidada reúne em um único documento todo o histórico de alterações contratuais passadas, tornando-se um documento independente dos contratos anteriores.

2.1.7 Prova de inscrição no cadastro de contribuintes estadual ou municipal, se houver, relativo ao domicílio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

2.1.8 Prova de regularidade relativa a Tributos Federais e à Divida Ativa da União, emitida conforme Portaria Conjunta RFB / PGFN nº.1.751 de 02/10/2014.

2.1.9 Prova de regularidade para com a Fazenda Estadual, mediante apresentação de Certidão Negativa de Débitos e Tributos Estaduais, expedida pela Secretaria de Estado da Fazenda, do domicílio ou sede da proponente;

2.1.10 Prova de regularidade para com a Fazenda Municipal, mediante apresentação de Certidão Negativa de Tributos Municipais, expedida pela Secretaria Municipal da Fazenda, do domicílio ou sede da proponente;

2.1.11 Prova de regularidade relativa ao Fundo de Garantia por Tempo de Serviços (FGTS), demonstrando situação regular no cumprimento dos encargos sociais instituídos por lei;

2.1.12 Prova de regularidade junto a Justiça do Trabalho (Certidão Negativa de Débitos Trabalhistas - CNDT), demonstrando a situação regular no cumprimento dos encargos trabalhistas instituídos por lei.

2.1.13 Para as empresas constituídas em consórcio, deverá observar as normas constantes no art. 16 do Decreto nº 5.450/2005, nos seguintes requisitos:

- 2.1.13.1 Comprovação da existência de compromisso público ou particular de constituição de consórcio, subscrito pelos consorciados;
- 2.1.13.2 Obrigatoriedade de liderança por empresa brasileira no consórcio formado por empresas brasileiras e estrangeiras;
- 2.1.13.3 Indicação da empresa líder que deverá conduzir o procedimento na licitação, além de ofertar lances, realizar negociação, responderá ainda, por todas as obrigações contratuais previstas neste Termo e seus anexos;
- 2.1.13.4 As empresas consorciadas deverão apresentar toda a documentação de habilitação exigida neste Termo;
- 2.1.13.5 Demonstração, pelas empresas, do atendimento aos índices contábeis definido no edital, para fins de qualificação econômico-financeira;
- 2.1.13.6 As empresas consorciadas não poderão participar, na mesma licitação, de mais de um consórcio ou isoladamente;
- 2.1.13.7 Caso vencedora da licitação, promover, antes da celebração do contrato, a constituição e o registro do consórcio;
- 2.1.13.8 As empresas consorciadas serão solidariamente responsáveis pelas obrigações do consórcio nas fases de licitação e durante toda a vigência do contrato que vier a ser assinado.

2.1.14 **Índices financeiros**:

2.1.14.1 A proponente deverá comprovar, por meio do **Modelo V**, sua capacidade financeira mediante a apresentação dos índices de liquidez geral (**LG**), liquidez corrente (**LC**) Solvência Geral (**SG**), apresentados com no máximo 02 (duas) casas decimais, cujos valores deverão ser iguais ou maiores que **1,0** (um). Tais índices serão calculados conforme segue:

LG = (AC + RLP) / (PC + ELP)
LC = (AC / PC)
SG = (AT) / (PC + ELP)

Onde:

AC - Ativo Circulante; **RLP** - Realizável a Longo Prazo;
PC - Passivo Circulante; **ELP** - Exigível a Longo Prazo.
AT - Ativo Total.

2.1.14.2 As empresas que apresentarem resultado inferior em qualquer dos índices referidos no subitem anterior, como condição de habilitação, deverão comprovar patrimônio líquido mínimo de 10% (dez por cento) do valor estimado da contratação, na forma prevista nos §§ 2º e 3º, do artigo 31, da Lei nº 8.666/93.

2.1.15 Certidão Negativa de Falência, recuperação judicial e extrajudicial, expedida pelo Cartório Distribuidor da sede da pessoa jurídica, expedida no domicílio da pessoa jurídica;

2.1.16 Balanço patrimonial e demonstrações contábeis do último exercício social, já exigíveis e apresentados na forma da lei, que comprovem a boa situação financeira da proponente, vedada a substituição por balancetes ou balanços provisórios. O Balanço e demonstrações a serem apresentados deverão ser cópia extraída do Livro Diário, com apresentação do Termo de Abertura e Encerramento deste, devidamente registrado na Junta Comercial do Estado ou órgão equivalente. Em se tratando de sociedade por ações (SA), deverá ser apresentada à publicação em órgão de imprensa oficial;

2.1.17 Comprovação da qualificação técnica:

2.1.1.17.1 A licitante deverá comprovar a sua qualificação e experiência para execução dos serviços descritos neste Termo de Referência, objeto desta licitação, com acervo seu, em características e quantitativos semelhantes aos especificados no edital, através da apresentação de, no mínimo, 01 (um) atestado de capacidade técnica, fornecido por pessoa jurídica de direito público ou privado, que deverá ser compatível, no mínimo, com o objeto desta licitação, ou seja, comprovando a experiência em: prestação dos serviços de fornecimento e implantação de solução para segurança e conectividade da área de Tecnologia da Informação (*hardwares* - equipamentos e *softwares* - sistemas).

2.1.1.17.2 A licitante deverá comprovar a sua qualificação e experiência para execução dos serviços descritos neste Termo de Referência, objeto desta licitação, com acervo seu, em características e quantitativos semelhantes aos especificados no edital,

através da apresentação de, no mínimo, 01 (um) atestado de capacidade técnica, fornecido por pessoa jurídica de direito público ou privado, que deverá ser compatível, no mínimo, com o objeto desta licitação, ou seja, comprovando a experiência em: prestação dos serviços de fornecimento de solução de backup com Serviços de Instalação, Migração de Ambiente, Ativação e Transferência de tecnologia.

2.1.1.17.3 A licitante deverá comprovar a sua qualificação e experiência para execução dos serviços descritos neste Termo de Referência, objeto desta licitação, com acervo seu, em características e quantitativos semelhantes aos especificados no edital, através da apresentação de, no mínimo, 01 (um) atestado de capacidade técnica, fornecido por pessoa jurídica de direito público ou privado, que deverá ser compatível, no mínimo, com o objeto desta licitação, ou seja, comprovando a experiência em: prestação dos serviços de fornecimento de Solução de Virtualização com Serviços de Instalação, Migração de Ambiente, Ativação e Transferência de tecnologia.

2.1.1.17.4 Os atestados deverão conter, no mínimo, as seguintes informações:

- O contratante com o seu endereço e CNPJ;
- A descrição do objeto da contratação;
- Período de realização dos serviços;
- Manifestação expressa do Contratante de que a Proponente "atende/eu satisfatoriamente ao contratado"* ou manifestação do grau de satisfação do cliente (ex: bom, ótimo ou excelente)*, em relação aos serviços prestados.
- *Não serão considerados os Atestados que contenham ressalvas;*

2.1.1.17.5 Havendo dúvidas quanto a regularidade ou inconsistências dos atestados, a Comissão realizará diligência para verificação destes, ou exigir outros documentos para comprovação (*Contrato de Prestação de Serviços e/ou Nota Fiscal*), na forma prevista no artigo 43, §3° da Lei 8.666/93. Recomenda-se que licitante envie o Contrato de Prestação de Serviços ou Notas Fiscais que comprovem a realização dos serviços;

2.1.1.17.6 Se apurado irregularidade na apresentação de qualquer documento apresentado na licitação, poderá ensejar a aplicação da penalidade prevista no artigo 7° da Lei 10.520/02 e o envio da documentação da licitante ao Ministério Público, para as providências que julgarem necessárias.

3. ENCAMINHAMENTO DA DOCUMENTAÇÃO AO PREGOEIRO

3.1. Após o encerramento da "Sessão Pública", a empresa arrematante deverá encaminhar, a proposta comercial e a documentação de habilitação, que deverão chegar até o Pregoeiro no prazo máximo de 03 (três) dias úteis posteriores à data do encerramento da Sessão Pública do Pregão, independente de comunicação do Pregoeiro.

3.2 Os documentos deverão chegar ao endereço constante do preâmbulo deste edital, sob pena de desclassificação da proposta, além das demais penalidades previstas neste edital, no prazo máximo de 03 (três) dias úteis posteriores à data do encerramento da Sessão Pública do Pregão, independente de comunicação do Pregoeiro.

3.3 O Pregoeiro poderá solicitar a documentação das empresas classificadas em segundo e terceiro lugares, e assim sucessivamente, para garantir a execução do objeto dentro das exigências do Edital. As empresas convocadas que não apresentarem a documentação estarão sujeitas às penalidades previstas neste Edital.

3.4 A licitante poderá encaminhar o envelope contendo os documentos habilitatórios anteriormente à realização da sessão do pregão, identificando no referido envelope os elementos que possibilitem seu vínculo ao processo licitatório. O Pregoeiro deverá abrir o envelope somente após a realização da sessão do Pregão. Os envelopes dos licitantes que não vencerem quaisquer dos itens deste edital estarão à disposição dos mesmos para sua retirada durante 60 (sessenta) dias após a realização da sessão, findo esse prazo serão destruídos.

4. CONSIDERAÇÕES SOBRE A DOCUMENTAÇÃO

4.1. Caso as Certidões não provem a regularidade do licitante, estes estarão imediatamente inabilitados no presente processo licitatório, além de sofrerem as penalidades previstas no edital e na legislação pertinente.

4.2. Os documentos referidos nos itens **2** e **3** deste Anexo poderão ser apresentados em original, cópia autenticada ou publicação em órgão da imprensa oficial. A aceitação das certidões, quando emitidas através da Internet, fica condicionada à verificação de sua validade sendo dispensada sua autenticação.

4.3. A documentação de que trata os itens **2** e **3** deste Anexo deverá estar dentro do prazo de validade no último dia previsto para a entrega da documentação e das propostas. Não será permitida documentação incompleta, protocolo ou quaisquer outras formas de comprovação que não sejam as exigidas neste Edital. **Não serão** aceitas **certidões que contenham ressalvas de que "não são válidas para fins licitatórios".**

4.4. Caso os documentos referidos nos itens **2** e **3** deste Anexo não mencionem o prazo de validade, será considerado o prazo de 60 (sessenta) dias contados de sua emissão.

4.5. Caso a licitante seja a matriz, todos os documentos apresentados deverão estar em nome da matriz. Caso seja a filial, todos os documentos deverão estar em nome da filial, exceto aqueles que, pela própria natureza ou por determinação legal, forem comprovadamente emitidos apenas em nome da matriz ou cuja validade abranja todos os estabelecimentos da empresa.

4.6. **As microempresas e empresas de pequeno porte deverão apresentar toda a documentação exigida para efeito de comprovação de regularidade fiscal, mesmo que esta apresente alguma restrição**. Havendo alguma restrição nos documentos de regularidade fiscal da microempresa ou empresa de pequeno porte, será assegurado o prazo de 05 (cinco) dias úteis para a regularização da documentação, sob pena de decair do direito à contratação.

4.7. Tratando-se de microempresa e empresa de pequeno porte, tendo em vista o tratamento diferenciado concedido pela Lei Complementar nº 123/2006, deverá apresentar a Certidão expedida pela Junta Comercial, conforme consta no art. 8º da Instrução Normativa DNRC nº 103/2007, e/ou declaração - **modelo I**, de que se enquadra como Microempresa ou Empresa de Pequeno Porte nos termos do art. 3º, da Lei Complementar n.º 123/06.

4.8. Ultrapassado o prazo previsto no subitem 4.6, a microempresa ou empresa de pequeno porte decairá do direito à contratação, sem prejuízo das sanções prevista na Lei Federal nº 8.666/93, sendo facultado à Administração convocar o licitante remanescente, na ordem de classificação para a assinatura do contrato ou revogar a licitação.

MODELO I

DECLARAÇÃO DE CUMPRIMENTO DOS REQUISITOS DA LEI COMPLEMENTAR Nº 123/06

A
Prefeitura Municipal de Foz do Iguaçu
Diretoria de Compras e Suprimentos
Pregão Eletrônico nº ____/2018.

A empresa _____, inscrita no CNPJ nº_____, por intermédio de seu representante legal o(a) Sr(a)_____, portador(a) da Carteira de Identidade nº_____ e do CPF nº _____, declara, que se enquadra na condição de Microempresa (ME) ou empresa de pequeno porte (EPP) constituídas na forma da Lei Complementar nº. 123, de 14/12/2006.

Declara, ainda que não apresenta nenhuma das restrições do regime diferenciado e favorecido, dispostas no art. 3º, § 4º, da referida Lei, **comprometendo-se a informar a Administração caso perca essa qualificação.**

Por ser verdade, firmamos a presente.

Local, ___ de _____ 2018.

_____
Nome e carimbo do representante
legal da empresa

_____
Contador:
Registro no CRC

MODELO II
DECLARAÇÃO CONJUNTA

A
Prefeitura Municipal de Foz do Iguaçu
Diretoria de Compras e Suprimentos
Pregão Eletrônico nº ____/2018.

A empresa _____, inscrita no CNPJ n° _____, por intermédio de seu representante legal o (a) Sr(a)_____, portador(a) do RG nº_____ e do CPF nº. _____, para fins do disposto no Edital de licitação em epigrafe, **declara**,

a) Que tomou conhecimento de todas as informações e condições para o cumprimento das obrigações objeto da licitação;
b) Que se sujeita às condições estabelecidas no edital do Pregão Eletrônico em consideração e dos respectivos anexos e documentos, que acatará integralmente qualquer decisão que venha a ser tomada pelo licitador quanto à habilitação apenas das proponentes que hajam atendido às condições estabelecidas e demonstrem integral possibilidade de executar os serviços;
c) Que inexistem fatos supervenientes impeditivos da habilitação ou que comprometam a idoneidade da proponente nos termos do art. 32, parágrafo 2°, e art. 97 da Lei 8.666/93 e suas alterações.
d) Que não emprega menor de dezoito anos em trabalho noturno, perigoso ou insalubre e não emprega menor de dezesseis anos em qualquer trabalho, salvo na condição de aprendiz a partir de 14 anos, conforme disciplina do art. 7º, XXXIII da CF 88;
e) Que não possui, empregados executando trabalho degradante ou forçado (incisos III e IV do art. 1º e no inciso III do art. 5º da CF/88);
f) Que não possui em seu quadro societário e nem como representante legal através de procuração, Servidor Público da Prefeitura de Foz do Iguaçu.

Por ser verdade, firmamos a presente.

Local, ___de _____2018.

_____
Nome e carimbo do Representante
Legal da empresa

MODELO III
DECLARAÇÃO DE ELABORAÇÃO INDEPENDENTE DE PROPOSTA

A
Prefeitura Municipal de Foz do Iguaçu
Diretoria de Compras e Suprimentos
Pregão Eletrônico nº ___/2018.

_____(***Identificação completa do representante da licitante***)_____, como representante devidamente constituído de (Identificação completa da licitante) doravante denominado Licitante, para fins do disposto no Edital de Pregão Eletrônico nº ____/2016, declara, sob as penas da lei, em especial o art. 299 do Código Penal Brasileiro, que:

a) a proposta apresentada para participar da presente Licitação, foi elaborada de maneira independente pelo Licitante, e o conteúdo da proposta não foi, no todo ou em parte, direta ou indiretamente, informado, discutido ou recebido de qualquer outro participante potencial ou de fato da Licitação, por qualquer meio ou por qualquer pessoa;

b) a intenção de apresentar a proposta elaborada para participar da presente Licitação não foi informada, discutida ou recebida de qualquer outro participante potencial ou de fato da Licitação, por qualquer meio ou por qualquer pessoa;

c) que não tentou, por qualquer meio ou por qualquer pessoa, influir na decisão de qualquer outro participante potencial ou de fato da Licitação quanto a participar ou não da referida licitação;

d) que o conteúdo da proposta apresentada para participar da presente Licitação não será, no todo ou em parte, direta ou indiretamente, comunicado ou discutido com qualquer outro participante potencial ou de fato da Licitação antes da adjudicação do objeto da referida licitação;

e) que o conteúdo da proposta apresentada para participar da presente Licitação não foi, no todo ou em parte, direta ou indiretamente, informado, discutido ou recebido de qualquer integrante da Prefeitura Municipal de Foz do Iguaçu antes da abertura oficial das propostas; e

f) que está plenamente ciente do teor e da extensão desta declaração e que detém plenos poderes e informações para firmá-la.

Por ser verdade, firmamos a presente.

Local, ___ de _____ de 2018.

_____
Nome e carimbo do representante
legal da empresa

MODELO IV

PROPOSTA DE PREÇOS
(*razão social, endereço, telefone, "e-mail" e CNPJ/MF*)

Local, ___ de _____ de 2018.

À
Prefeitura Municipal de Foz do Iguaçu
Diretoria de Compras e Suprimentos
Pregão Eletrônico nº ____/2018.

Prezados Senhores,

Apresentamos e submetemos à apreciação de V. S^as^ nossa proposta de preços relativa à execução _____ (*inserir o objeto da licitação*) _____, da licitação em epígrafe.

O preço global, fixo e sem reajuste, proposto para execução do objeto é de R$_____ (_____).

O prazo de execução do objeto é de ___ (_____) dias.

O prazo de validade da proposta de preços é de 60 (sessenta) dias contados a partir da data do recebimento das propostas pela Comissão de Licitação.

Declaramos que em nossos preços estão inclusos todos os custos diretos e indiretos para a perfeita execução do objeto da licitação, tais como materiais, mão de obra, equipamentos, encargos sociais, trabalhistas e previdenciários, administração, lucro e qualquer outra despesa incidentes ou que venha a incidir, sobre o objeto do referido no convite.

Na execução do objeto licitado, observaremos, rigorosamente, as especificações das normas técnicas brasileiras ou qualquer outra que garanta a qualidade igual superior, assumindo, desde, já a integral responsabilidade pela perfeita realização dos trabalhos.

_____
(*carimbo, nome e assinatura do responsável legal*)
(*carteira de identidade, número e órgão emissor*)

MODELO V

CAPACIDADE FINANCEIRA

À
Prefeitura Municipal de Foz do Iguaçu
Diretoria de Compras e Suprimentos
Pregão Eletrônico nº ___/2018.

Prezados Senhores:

Declaramos que as demonstrações abaixo correspondem a real situação da proponente. Esses índices foram obtidos no balanço do ultimo exercício social.

Declaramos, ainda, que a qualquer tempo, desde que solicitado pelo licitador, nos comprometemos a apresentar as demonstrações financeiras que comprovarão as demonstrações.

SÃO AS DEMONSTRAÇÕES:

Tipo de índice	Valor em reais	Índice
Liquidez geral (LG) LG = (AC + RLP) / (PC + ELP)		
Liquidez corrente (LC) LC = AC / PC		
Solvência Geral (SG) SG= (AT) / (PC + ELP)		

Onde:

AC - Ativo Circulante; AT - Ativo Total;
PC - Passivo Circulante; RLP - Realizável a Longo Prazo;
ELP - Exigível a Longo Prazo.

Obs. Os índices deverão ser apresentados com no máximo 2 (duas) casas decimais, desprezando-se as demais.

Local, ___ de _____ de 2018.

Responsável legal
(Carimbo, nome RG nº e assinatura)

Contador
(nome, RG nº, CRC nº e assinatura)

ANEXO III - MINUTA DE CONTRATO

O MUNICÍPIO DE FOZ DO IGUAÇU, Estado do Paraná, pessoa jurídica de direito público interno, com sede à Praça Getúlio Vargas nº 280, inscrita sob o CNPJ/MF nº 76.206.606/0001-40, neste ato representado pelo Prefeito Municipal, Senhor Francisco Lacerda Brasileiro, a seguir denominado CONTRATANTE e, de outro lado,_____, pessoa jurídica, inscrita no CNPJ/MF sob o nº _____, com sede na _____, nº _____, na cidade de _____, neste ato representada pelo Sr _____, portador da Cédula de Identidade nº_____ e do CPF nº _____, residente e domiciliado na cidade de _____, a seguir denominada CONTRATADA, têm entre si justo e contratada o constante nas cláusulas a seguir enumeradas:

CLÁUSULA PRIMEIRA - DO OBJETO

O presente contrato tem por objeto a prestação dos serviços de fornecimento e implantação de solução de segurança e conectividade (*hardwares* - equipamentos e *softwares* - sistemas) para as áreas de tecnologia da informação da Prefeitura Municipal de Foz do Iguaçu, incluindo-se o fornecimento de equipamentos e sistemas necessários para a ampliação e/ou a substituição de ativos de rede, *internet*, *firewall*, *switches* e roteadores, bem como *softwares* e demais sistemas necessários, conforme descrição e quantitativos estabelecidos neste Termo de Referência e seus anexos, os quais a CONTRATADA se declara em condições de prestar os serviços em estrita observância com o indicado nas especificações e na documentação levada a efeito pelo Pregão Eletrônico nº. ____/2018.

CLÁUSULA SEGUNDA - DA CONTRATAÇÃO

Ficam integrados a este Contrato, independente de transcrição, os seguintes documentos cujos teores são de conhecimento da CONTRATADA: atos convocatório, edital de licitação, especificações e memoriais, proposta da proponente vencedor, parecer de julgamento e legislação pertinente à espécie.

Parágrafo Primeiro

Será incorporada a este contrato, mediante Termos Aditivos, qualquer modificação que venha a ser necessária durante a sua vigência, decorrente das obrigações assumidas pela CONTRATADA, alterações no objeto, especificações, prazos ou normas gerais de serviços do CONTRATANTE.

Parágrafo Segundo

A assinatura do presente contrato indica que a CONTRATADA possui plena ciência de seu conteúdo, bem como dos demais documentos vinculados ao presente, sujeitando-se às normas da Lei 8.666/93 e a totalidade das cláusulas contratuais aqui estabelecidas.

Parágrafo Segundo

A CONTRATADA poderá requerer o reajuste de seu contrato anualmente tendo como base os índices oficiais de inflação ou a qualquer tempo no caso do comprovado desequilíbrio

econômico e financeiro do CONTRATO em virtude da ocorrência de algum evento que se enquadre na alínea "d" do inciso II do artigo 65 da Lei 8.666/93.

CLÁUSULA TERCEIRA - DO VALOR CONTRATUAL

A CONTRATANTE pagará à CONTRATADA, pela prestação dos serviços, o valor global de R$_____(_____), que serão empenhados a conta das seguintes dotações:

12.01.12.361.0120.1030.449052.3500.1.104 / 12.03.12.361.0600.2114.339039.9400.1.103;
14.02.04.126.0140.1040.449052.3500.1.505 / 14.02.04.126.0140.1040.339039.9400.1.505;
10.01.10.122.0100.2090.339039.9400.1.000 / 10.01.10.122.0100.2090.449052.3500.1.303;
08.05.08.244.0080.1016.449052.3500.1.505 / 08.05.08.244.0510.1015.449052.3500.1.505.

CLÁUSULA QUARTA - DA FORMA DE:

Os pagamentos serão efetuados, mediante apresentação da Nota Fiscal Eletrônica, com as especificações de cada medição, em até 30 (trinta) dias após a realização do(s) serviço(s), observados o cronograma do Anexo I - Termo de Referência, vedada a sua antecipação;

O faturamento deverá ser apresentado e protocolado, em uma via original, no protocolo geral na sede da contratante;

Para recebimento dos pagamentos devidos, o fornecedor deverá apresentar junto à Secretaria Municipal da Fazenda, os seguintes documentos:

Prova de regularidade relativa a Tributos Federais e à Divida Ativa da União, emitida conforme Portaria Conjunta RFB / PGFN nº.1.751 de 02/10/2014.

Prova de regularidade para com a Fazenda Estadual, mediante apresentação de Certidão Negativa de Débitos e Tributos Estaduais para participar de licitação junto a órgãos públicos, expedida pela Secretaria de Estado da Fazenda, do domicílio ou sede da proponente;

Prova de regularidade para com a Fazenda Municipal, mediante apresentação de Certidão Negativa de Tributos Municipais, expedida pela Secretaria Municipal da Fazenda, do domicílio ou sede da proponente;

Prova de regularidade relativa ao Fundo de Garantia por Tempo de Serviços (FGTS), demonstrando situação regular no cumprimento dos encargos sociais instituídos por lei;

Prova de regularidade junto a Justiça do Trabalho, mediante a apresentação da Certidão Negativa de Débitos Trabalhistas, demonstrando a situação regular no cumprimento dos encargos trabalhistas instituídos por lei.

É obrigatória a emissão de Nota Fiscal de Prestação de Serviços Eletrônica, na forma contida no Decreto Municipal nº 21.524 de 02 de Agosto de 2012, expedida em conformidade com a legislação federal (Protocolo ICMS 42/2009).

CLÁUSULA QUINTA - DO PRAZO DE EXECUÇÃO DO CONTRATO

O prazo de execução dos serviços será de 12 (doze) meses, contados a partir da data da assinatura, podendo ser prorrogado por iguais períodos nas mesmas condições iniciais, conforme disposto no artigo 57, II, da Lei nº. 8.666/93 e alterações posteriores.

CLÁSULA SEXTA - DAS OBRIGAÇÕES DA CONTRATADA

Prestar os serviços, entregar e instalar os equipamentos que compõem a solução de segurança e conectividade, objeto deste Termo de Referência, de acordo com as especificações e quantidades descritas;

A empresa deverá possuir equipe técnica de pessoal, própria, para execução do contrato;

Responder, em relação aos seus empregados, por todas as despesas decorrentes dos serviços, tais como: salários, seguros de acidentes, tributos, indenizações, vales refeição, vale-transporte e outras que porventura venham a ser regulada em acordo coletivo;

A Prefeitura Municipal de Foz do Iguaçu não se responsabilizará por qualquer despesa de responsabilidade do fornecedor ou correspondente aos técnicos alocados, como transporte, alimentação, salários, seguros de vida, etc.;

Executar diretamente o contrato, sem a transferência de responsabilidades ou subcontratações não autorizadas pela Prefeitura Municipal de Foz do Iguaçu;

Selecionar e treinar os empregados que irão prestar os serviços, tendo funções profissionais legalmente registradas em suas carteiras de trabalho;

Responder pelos danos causados diretamente a Prefeitura Municipal de Foz do Iguaçu ou a terceiros, decorrentes de sua culpa ou dolo;

Manter, os seus empregados uniformizados e identificados por crachá, quando em trabalho, devendo substituir imediatamente qualquer um deles que seja considerado inconveniente à boa ordem e às normas disciplinares da Prefeitura Municipal de Foz do Iguaçu;

Respeitar as normas e procedimentos de controle e acesso às dependências da Prefeitura Municipal de Foz do Iguaçu;

Arcar com despesas decorrentes de qualquer infração, seja qual for, desde que praticada por seus empregados, quando relacionados com a execução dos serviços;

Comunicar por escrito, a Prefeitura Municipal de Foz do Iguaçu, qualquer anormalidade verificada na execução dos serviços, relatando-as no Livro de Ocorrências, com os danos e circunstâncias julgados necessários ao relato e esclarecimento dos fatos;

Observar o horário de trabalho estabelecido pela Prefeitura Municipal de Foz do Iguaçu, em conformidade com as leis trabalhistas;

Manter, durante a execução do contrato as condições que ensejaram a contratação;

Informar ao Ministério Público a ocorrência de qualquer irregularidade ocorrida com os técnicos alocados;

Emitir e enviar, à Prefeitura Municipal de Foz do Iguaçu, notas fiscais de serviços (NFS-e) ou de aquisição de equipamentos (NF-e) de acordo com o cronograma de pagamentos pré-estabelecido em até 48 (quarenta e oito horas) após a entrega dos mesmos e aceite da PMFI/SMTI;

No valor da proposta deverão estar incluídos todos os encargos sociais, impostos, tributos, taxas, etc., inclusive aqueles que deverão ser recolhidos aos cofres do município.

CLÁSULA SÉTIMA - DAS OBRIGAÇÕES DA CONTRATANTE

Efetuar o pagamento devido pela prestação dos serviços de implantação da solução pretendida, bem como pelo fornecimento e instalação dos equipamentos, desde que cumpridas todas as formalidades e exigências do contrato;

Sendo necessário, permitir o livre acesso dos empregados da licitante vencedora as dependências dos órgãos que compõem a administração pública do Governo Municipal, para execução dos serviços ora contratados, desde que devidamente identificados;

Prestar as informações e os esclarecimentos que venham a ser solicitado pelos empregados da licitante vencedora;

Comunicar a licitante vencedora, quaisquer irregularidades ocorridas, consideradas de natureza grave;

Solicitar, quando necessário, treinamentos ou substituições dos técnicos alocados;

Exercer a gestão, fiscalização, orientação e distribuição dos serviços, através da PMFI/SMTI, acompanhando a execução do contrato através de gestor e fiscal, devidamente investido;

Atestar as faturas correspondentes, pela SMTI.

CLAUSULA OITAVA - DA FISCALIZAÇÃO

A fiscalização e o acompanhamento do objeto deste Contrato será feita pelo CONTRATANTE, através de profissionais qualificados e indicado pelo órgão requisitante. Serão designados os seguintes profissionais para fiscalização e gestão do objeto contratual:

GESTOR do contrato:

- **Nome:** Evandro Ferreira -
- **Cargo/Função**: Secretário Municipal de Tecnologia da Informação.

FISCAL do contrato:

- **Nome:** Sandro Lopes Ebbing;
- **Cargo/Função:** Diretor De Infraestrutura e Segurança da Informação.

CLAUSULA NONA - DA GARANTIA DE EXECUÇÃO

A proponente vencedora, no prazo de 10 (dez) dias após a assinatura do Contrato, deverá, sob pena de decair o direito de contratação, apresentar comprovação de formalização da garantia de execução, que servirá de garantia à fiel observância das obrigações contratuais.

O valor da garantia de execução será obtido pela aplicação de 5% (cinco por cento) sobre o valor contratual;

Qualquer majoração do valor contratual obrigará a contratada a depositar, nas mesmas modalidades dos itens anteriores, valor correspondente a 5% (cinco por cento) do valor da alteração ou alterar o valor do título de garantia de cumprimento no mesmo montante da majoração do contrato, que fará parte integrante da garantia de execução. No caso de redução do valor contratual, poderá a contratada ajustar o valor da garantia de execução, se assim o desejar;

No caso de inadimplência das obrigações e/ou rescisão do contrato com fundamento no artigo 78, incisos I a XI será descontada da garantia de execução os prejuízos acarretados à contratante;

A devolução da garantia de execução se houver, ou o valor que delas restar, dar-se-á mediante a apresentação do Termo de recebimento definitivo.

CLÁUSULA DÉCIMA - DA CESSÃO DO CONTRATO E SUBCONTRATAÇÃO

A CONTRATADA não poderá ceder o presente Contrato a nenhuma pessoa física ou jurídica, sem autorização prévia, por escrito, do CONTRATANTE.

CLÁUSULA DÉCIMA PRIMEIRA - DA FRAUDE E DA CORRUPÇÃO

O CONTRATADO deve e fazer observar, por seus fornecedores e subcontratados, se admitida subcontratação, o mais alto padrão de ética durante todo o processo de contratação e de execução do objeto contratual. Para os propósitos desta cláusula, definem-se as seguintes práticas:

a) *Prática corrupta: oferecer, dar, receber ou solicitar, direta ou indiretamente, qualquer vantagem com o objetivo de influenciar a ação de servidor público no processo de licitação ou na execução de contrato;*
b) *Prática fraudulenta: a falsificação ou omissão dos fatos, com o objetivo de influenciar o processo de licitação ou de execução de contrato;*
c) *Prática colusiva: esquematizar ou estabelecer um acordo entre dois ou mais licitantes, com ou sem o conhecimento de representantes ou prepostos do órgão licitador, visando estabelecer preços em níveis artificiais e não competitivos;*
d) *Prática coercitiva: causar dano ou ameaçar causar dano, direta ou indiretamente, às pessoas ou sua propriedade, visando influenciar sua participação em um processo licitatório ou afetar a execução do contrato.*
e) *Prática obstrutiva: (i) destruir, falsificar, alterar ou ocultar provas em inspeções ou fazer declarações falsas aos representantes do organismo financeiro multilateral, com o objetivo de impedir materialmente a apuração de alegações de prática prevista neste Edital; (ii) atos cuja intenção seja impedir materialmente o exercício do direito de o organismo financeiro multilateral promover inspeção.*

CLÁUSULA DÉCIMA SEGUNDA - DA SEGURANÇA E DA RESPONSABILIDADE CIVIL DA CONTRATADA

A CONTRATADA responderá pela solidez do objeto deste contrato, nos termos do artigo 618 do Código Civil Brasileiro, bem como pelo bom andamento dos serviços, podendo o CONTRATANTE, por intermédio da fiscalização, impugná-los quando contrariarem a boa técnica ou desobedecerem as especificações.

Parágrafo Primeiro

A CONTRATADA assumirá integral responsabilidade por danos causados ao CONTRATANTE ou a terceiros decorrentes da execução dos serviços ora contratados, inclusive acidentes, mortes, perdas ou destruições parciais ou totais, isentando O CONTRATANTE de todas as reclamações que possam surgir com relação ao presente Contrato.

Parágrafo Segundo

Também, obriga-se a CONTRATADA a reparar, corrigir, reconstruir ou substituir às suas expensas, no total ou em parte, o objeto do Contrato em que se verificarem defeitos, vícios ou incorreções resultantes da execução ou de materiais empregados.

Parágrafo Terceiro

Caso a CONTRATANTE seja acionada judicial ou administrativamente, inclusive reclamações trabalhistas, por qualquer ato decorrente do presente Contrato, a CONTRATADA assumirá para si a responsabilidade por toda e qualquer eventual condenação, isentando a CONTRATANTE de quaisquer obrigações, aplicando-se no caso concreto uma das formas de intervenção de terceiros previstas no Código de Processo Civil, especialmente a denunciação da lide (art. 70 - CPC), se for o caso.

Parágrafo Quarto

A intenção das partes, aqui manifestada expressamente, é a de que a CONTRATADA assuma e se responsabilize direta e integralmente pela plena e total realização dos serviços contratados, sob pena de incorrer em descumprimento de obrigação contratual e sujeitar-se à aplicação das penalidades cabíveis.

Parágrafo Quinto

A CONTRATADA responde, exclusiva e diretamente, por todo e qualquer ato ilícito praticado por seus prepostos que dele decorra a obrigação e/ou necessidade de ressarcimento de danos materiais ou morais (art. 932, III, Código Civil), não podendo a CONTRATANTE ser responsabilizada por eles a nenhum título.

CLÁUSULA DÉCIMA TERCEIRA - PENALIDADES PELA INEXECUÇÃO DO OBJETO

Pela inexecução total ou parcial do contrato, a Administração poderá aplicar à CONTRATADA, as seguintes sanções:

I. Advertência;
II. Multa, na forma prevista no instrumento convocatório;
III. Impedimento de contratar com a Administração, por prazo não superior a 2 (dois) anos;
IV. Declaração de inidoneidade para licitar ou contratar com a Administração Pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que o contratado ressarcir a Administração pelos prejuízos resultantes e após decorrido o prazo da sanção aplicada com base no inciso anterior.

CLÁUSULA DÉCIMA QUARTA - DA APLICAÇÃO DAS MULTAS

Quando da aplicação de multas, O CONTRATANTE notificará à CONTRATADA que terá prazo de 10 (*dez*) dias para recolher à Tesouraria do CONTRATANTE a importância correspondente, sob pena de incorrer em outras sanções cabíveis.

As sanções previstas nesta cláusula inclusive poderão cumular-se e não excluem a possibilidade de rescisão administrativa do Contrato;

A multa será cobrada pelo CONTRATANTE de acordo com o estabelecido pela legislação pertinente.

Compete à CONTRATANTE, quando for o caso, por proposta da fiscalização, a aplicação de multas, tendo em vista a gravidade da falta cometida pela CONTRATADA;

Da aplicação de multas, caberá recurso à Contratada no prazo de 03 (três) dias, a contar do recebimento da respectiva notificação, mediante prévio recolhimento da multa, sem efeito suspensivo. O Contratante julgará, no prazo máximo de 30 (trinta) dias procedente ou improcedente a penalidade a ser imposta, devendo fundamentá-la e, se improcedente, a importância recolhida pela CONTRATADA será devolvida pelo Contratante, no prazo de 03 (três) dias, contados da data do julgamento.

CLÁUSULA DÉCIMA QUINTA - DA RESCISÃO

O CONTRATANTE reserva-se o direito de rescindir o Contrato, independentemente de interpelação judicial ou extrajudicial, sem que à CONTRATADA caiba o direito de indenização de qualquer espécie, nos seguintes casos: (a) quando a CONTRATADA falir ou for dissolvida; (b) quando a CONTRATADA transferir no todo ou em parte o Contrato sem a prévia anuência do CONTRATANTE.

§ 1º - A rescisão do Contrato na mesma forma prevista no caput, ocorrerá nas seguintes hipóteses:

I. Por ato unilateral escrito da Administração, nos casos enumerados nos incisos I a XII e XVII do artigo 78 da Lei 8.666/93;
II. Amigável, por acordo entre as partes, reduzida a termo no processo da licitação, desde que haja conveniência para a Administração;
III. Judicial, nos termos da legislação.

§ 2º - A rescisão do Contrato, quando motivada por qualquer dos itens acima relacionados, implicará a apuração de perdas e danos, sem embargos da aplicação das demais providências legais cabíveis.

§ 3º - O Contratante, por conveniência exclusiva e independentemente de cláusulas expressas, poderá rescindir o Contrato desde que efetue os pagamentos devidos, relativos ao mesmo.

CLÁUSULA DÉCIMA SEXTA - DOS CASOS OMISSOS

Os casos omissos e o que se tornar controvertido em face das presentes cláusulas contratuais, serão resolvidos administrativamente entre as partes, de acordo com a legislação pertinente.

CLÁUSULA DÉCIMA SÉTIMA - DO FORO

As partes contratantes ficam obrigadas a responder pelo cumprimento deste termo, perante o Foro da Comarca de Foz do Iguaçu, Estado do Paraná, não obstante qualquer mudança de domicílio da CONTRATADA que, em razão disso, é obrigada a manter um representante com plenos poderes para receber notificação, citação inicial e outras medidas em direito permitidas.

Justas e contratadas, firmam as partes este instrumento, em 02 (*duas*) vias de igual teor, a fim de que produza seus efeitos legais.

Foz do Iguaçu, ___ de _____ de 2018.

Francisco Lacerda Brasileiro
Prefeito Municipal

Evandro Ferreira
Secretário Mun. da Tecnologia da Informação

Contratada