PREGÃO ELETRÔNICO N.º 010/2017/IOE

A Imprensa Oficial do Estado – IOE, por meio do Pregoeiro nomeado pela **Portaria n.º 031 de 13 de março de 2017**, de acordo com a autorização constante do **Processo n.º 139/2017/IOE**, torna público para conhecimento dos interessados que na data, horário e sítio abaixo indicados fará realizar licitação na modalidade **PREGÃO ELETRÔNICO**, do tipo **MENOR PREÇO GLOBAL**, conforme descrito neste Edital e seus anexos.

O procedimento licitatório será regido, integralmente, pela Lei n.º 10.520, de 17 de julho de 2002, pelo Decreto n.º 3.555, de 08 de agosto de 2000, pelo Decreto n.º 5.450, de 31 de maio de 2005, pela Lei Estadual n.º 6.474/02, pelo Decreto Estadual n.º 0199/03 e pelo Decreto Estadual n.º 2.069, de 20 de fevereiro de 2006, aplicando–se, subsidiariamente, no que couber, a Lei n.º 8.666, de 21/06/93, com as respectivas alterações posteriores, cuja sessão de abertura dar-se-á de acordo com o que segue:

DATA: 19/05/2017
HORÁRIO DA ABERTURA DO CERTAME: 10:00 horas (horário de Brasília - DF)
SÍTIO: www.comprasnet.gov.br
E-MAIL: licitacao@ioe.pa.gov.br
FAC-SÍMILE: (91) 4009–7839
UASG: 925608

1 – DO OBJETO

1.1 A presente licitação tem por objeto a aquisição de serviço de segurança da informação, fornecendo e integrando firewalls UTM, firewalls de aplicação WEB, gestão de senhas de alto-privilégio e proteção contra ameaças avançadas (ANTI-RANSOMWARE), incluindo pacote, administração de largura de banda (QoS), VPN, IPSec, SSL e IPS, antivírus, anti-spyware, para atendimento às características técnicas mínimas descritas no projeto, com o fornecimento de hardware, software e solução em nuvem, serviços de instalação, configuração, suporte, avaliação de ambientes, monitoramento contínuo, repasse tecnológico e migração das regras de firewall atualmente implementadas para as novas soluções, conforme especificações constantes no Anexo II – Termo de Referência deste edital.

1.2 Em caso de **divergência entre as especificações do edital e as do Sistema Comprasnet, prevalecerão as do edital.**

2 – DA DOTAÇÃO ORÇAMENTÁRIA

2.1 As despesas decorrentes da aquisição do objeto da presente licitação correrão por conta da seguinte dotação orçamentária:

Fonte de Recurso: 0661.00.0000
Natureza da Despesa: 33.90.39
Programa de Trabalho: 22.131.1424.8233;
Plano Interno – 419.000.8233C
Fonte de Recurso: 0261.00.0000
Natureza da Despesa: 33.90.39
Programa de Trabalho: 22.131.1424.8233

Plano Interno – 419.000.8233C

3 – DAS CONDIÇÕES DE PARTICIPAÇÃO

3.1 Poderão participar deste Pregão Eletrônico, os interessados que atenderem a todas as exigências, inclusive
quanto à documentação, constantes deste Edital e seus anexos e que estejam obrigatoriamente cadastrados no Sistema de Cadastramento Unificado de Fornecedores – SICAF.

3.1.1 Os licitantes arcarão com todos os custos decorrentes da elaboração e apresentação de suas propostas.

3.2 Somente poderão participar deste Pregão Eletrônico, na condição de proponente:

3.2.1 Empresas em funcionamento no país, desde que desenvolvam atividade pertinente e compatível com o objeto desta licitação, comprovada por meio de Contrato Social ou documento equivalente.

3.3 Não poderão participar deste Pregão Eletrônico:

3.3.1 Empresas em recuperação judicial, extrajudicial ou em processo de falência, sob concurso de credores, em dissolução ou em liquidação;

3.3.2 Consórcio de empresas;

3.3.3 Empresas declaradas inidôneas para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade;

3.3.4 Cooperativas.

3.3.5 Empresas em processo falimentar, em processo concordatário, em recuperação judicial ou extrajudicial;

3.3.6 Quaisquer interessados que se enquadrem nas vedações previstas no artigo 9º da Lei n.º 8.666/93.

3.4 O licitante deverá manifestar, em campo próprio do sistema eletrônico, o pleno conhecimento e atendimento às exigências de habilitação previstas no Edital (art. 22, § 2º do Decreto Estadual n.º 2.069/2006).

3.5 Não será admitida a subcontratação, sob qualquer pretexto ou alegação.

4 – DO TRATAMENTO DAS MICROEMPRESAS, EMPRESAS DE PEQUENO PORTE E EQUIPARADOS

4.1 No caso de participação de microempresas, empresas de pequeno porte ou equiparados, será observado o disposto na Lei Complementar n.º 123/06, notadamente os arts. 42 a 49.

4.1.1 O enquadramento como microempresa - ME ou empresa de pequeno porte - EPP dar-se-á nas condições do Estatuto Nacional da Microempresa e Empresa de Pequeno Porte, instituído pela Lei Complementar n.º 123/06.

4.1.2 A pessoa física ou o empresário individual enquadrados nos limites definidos pelo art. 3º da Lei Complementar n.º 123/06 receberá o mesmo tratamento concedido pela Lei Complementar n.º 123/06, às ME/EPP.

4.2 A fruição dos benefícios licitatórios determinados pela Lei Complementar n.º 123/06 independe da habilitação da ME/EPP ou equiparado para a obtenção do regime tributário simplificado.

4.3 Os licitantes que se enquadrarem nas situações previstas no art. 3º da Lei Complementar n.º 123/06, e não possuírem quaisquer dos impedimentos do § 4º do artigo citado, deverão apresentar declaração em campo próprio do sistema que cumprem os requisitos legais para a qualificação como ME/EPP ou equiparado, estando aptos a usufruir do tratamento favorecido estabelecido nos arts. 42 a 49 da referida Lei Complementar n.º 123/06 (Art. 11 do Decreto n.º 6.204/07).
4.4 Caso inexistente campo próprio no sistema eletrônico, a declaração deverá ser enviada ao pregoeiro até a data e horário marcados para abertura da sessão.
4.5 A não apresentação da declaração de ME/EPP e equiparado importará na renúncia ao tratamento consagrado na Lei Complementar n.º 123/06.
4.6 A identificação das ME/EPP ou equiparados na sessão pública do pregão eletrônico só deverá ocorrer após o encerramento dos lances, de modo a impedir a possibilidade de conluio ou fraude no procedimento.

5 – DA REPRESENTAÇÃO E DO CREDENCIAMENTO
5.1 O credenciamento dar-se-á pela atribuição de chave de identificação e de senha, pessoal e intransferível, para acesso ao sistema eletrônico (art. 3º, § 1º do Decreto Estadual n.º 2.069/2006), no sítio COMPRASNET (**www.comprasnet.gov.br**).
5.2 O credenciamento junto ao provedor do sistema implica a responsabilidade legal do licitante ou de seu representante legal e a presunção de sua capacidade técnica para realização das transações inerentes ao Pregão Eletrônico (art. 3º, § 6º do Decreto Estadual n.º 2.069/2006).
5.3 O uso da senha de acesso pelo licitante é de sua responsabilidade exclusiva, incluindo qualquer transação efetuada diretamente ou por seu representante, não cabendo ao provedor do sistema ou à IOE responsabilidade por eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros (art. 14, inciso III do Decreto Estadual n.º 2.069/2006).
5.4 O credenciamento do licitante dependerá de registro cadastral atualizado no SICAF, que também será requisito obrigatório para fins de habilitação.
5.5 Cada credenciado poderá representar apenas um licitante.

6 – DAS PROPOSTAS DE PREÇOS
6.1 A participação no Pregão Eletrônico dar-se-á por meio da digitação da senha privativa do licitante e subsequente encaminhamento da Proposta de Preços (art. 22, §1º do Decreto Estadual n.º 2.069/2006).
6.2 A Proposta de Preços deverá ser encaminhada por meio do sistema eletrônico, a partir da data de liberação do Edital no sítio COMPRASNET (**www.comprasnet.gov.br**) até o horário-limite para o início da sessão pública, que se dará pela abertura das propostas no dia **19/05/2017, às 09:00h, horário de Brasília/DF** (art. 22 do Decreto Estadual n.º 2.069/2006).
6.3 O envio da Proposta de Preços deve se dar com o preenchimento dos campos próprios apresentados pelo sistema eletrônico no sítio COMPRASNET (**www.comprasnet.gov.br**).
6.4 O valor da Proposta de Preços deverá corresponder ao valor total do objeto, devendo englobar todas as despesas referentes ao fornecimento, bem como todos os tributos, frete até o destino (sede da IOE), implantação, treinamento, manutenção, encargos sociais e trabalhistas e quaisquer outras despesas e insumos que incidam ou venham a incidir sobre o objeto desta licitação.

6.4.1 A omissão de qualquer despesa necessária à perfeita execução do objeto desta licitação, inclusive quanto a entrega e/ou descarga, será interpretada como não existente ou já incluída no preço, não podendo a licitante pleitear acréscimos após a abertura das propostas.
6.4.2 A proposta de preços deve ser inserida no Sistema Comprasnet e deverá conter a descrição minuciosa do objeto ou serviço ofertado, devendo constar a marca, modelo e todos os detalhes de relevância do objeto.
6.4.2.1 Serão desclassificadas as propostas que se limitarem a simples transcrição da descrição do objeto conforme contido no Termo de Referência.
6.4.3 Ressalte-se que a simples descrição "Conforme o edital", ou expressões equivalentes, não cumprirá com tal exigência, sendo motivo de desclassificação da proposta comercial, por estar em desacordo com as normas editalícias.
6.5 No preenchimento da Proposta de Preços, o licitante deve informar os seguintes dados:
6.5.1 Preço de acordo com os valores praticados no mercado, em algarismo, com preenchimento em campo próprio, expresso em moeda nacional (R$).
6.5.2 Informar na proposta de preços a marca do produto a ser entregue.
6.5.3 Informar o nome do Banco, número da Agência e número da Conta Corrente para efeito de depósito referente ao pagamento, na forma do Decreto Estadual n.º 877, de 31 de março de 2008, publicado no DOE n.º 31.139, de 01/04/2008 e Instrução Normativa n.º 0018, de 21 de maio de 2008 da Secretaria de Estado da fazenda – SEFA, publicada no DOE n.º 31.174, de 23/05/2008.
6.5.4 Prazo para entrega do sistema e implantação do sistema obedecerá ao disposto no Termo de Referência (Anexo II).
6.5.5 Frete incluso (CIF Belém-PA).
6.6 O prazo de validade de Proposta de Preços apresentada é de 60 (sessenta) dias a contar da data de seu recebimento (art. 9º, inciso XXVIII da Lei Estadual n.º 6.474/2002, combinado com o art. 28, § 4º do Decreto Estadual n.º 2.069/2006).
6.7 Até a abertura da sessão, os licitantes poderão retirar ou substituir a proposta anteriormente apresentada (art. 22, § 4º do Decreto Estadual n.º 2.069/2006).
6.8 A oferta deverá ser precisa, sem alternativas de preços ou qualquer outra condição que induza o julgamento a ter mais de um resultado.
6.9 Não se considerará nenhuma oferta ou vantagem não prevista neste Edital.
6.10 Serão desclassificadas:
6.10.1 As propostas que não atendam às exigências ao ato convocatório da licitação;
6.10.2 As propostas que apresentarem valores unitários e/ou global, superiores ao limite estabelecido, tendo-se como limite estabelecido o orçamento estimado do serviço ou do objeto, ou ainda com preços unitários ou globais, manifestamente inexequíveis, assim considerados aqueles que não venham a ter demonstrado sua viabilidade através de documentação que comprove que os custos dos insumos são coerentes com os de mercado e que os coeficientes de produtividade são compatíveis com a execução do objeto do contrato, bem como aqueles que não atenderem ao Art. 44, Parágrafo 3º da Lei n.º 8.666/93.
6.10.3 As propostas que apresentem preços com cotação no valor zero, simbólicos e/ou irrisórios, incompatíveis com os preços praticados no mercado, exceto quando se referirem aos materiais e

instalações de propriedade do próprio licitante, para os quais ele renuncie a parcela ou à totalidade da remuneração.
6.11 Por ocasião da licitação, as empresas deverão levar em conta o modelo de proposta de preço, conforme contido no **ANEXO III**.

7 – DA ABERTURA DAS PROPOSTAS
7.1 A partir do horário previsto no preâmbulo deste Edital e, em conformidade com o subitem 6.2, terá início a sessão pública do **Pregão Eletrônico N.º 010/2017/IOE**, com a divulgação das Propostas de Preços recebidas conforme o Edital e de acordo com o Decreto Estadual n.º 2.069/2006.
7.2 O Pregoeiro verificará as propostas apresentadas, desclassificando aquelas que não estejam em conformidade com os requisitos estabelecidos no Edital (art. 23, § 2º do Decreto Estadual n.º 2.069/2006).
7.3 A desclassificação de proposta será sempre fundamentada e, registrada no sistema, com acompanhamento em tempo real por todos os participantes (art. 23, § 3º do Decreto Estadual n.º 2.069/2006).
7.4 As propostas contendo a descrição do objeto, valor e eventuais anexos estarão disponíveis na internet (art. 23, § 4º do Decreto Estadual n.º 2.069/2006).
7.5 O sistema disponibilizará campo próprio para troca de mensagens entre o Pregoeiro e os licitantes (art. 23, § 5º do Decreto Estadual n.º 2.069/2006).
7.6 O sistema ordenará, automaticamente, as propostas classificadas pelo Pregoeiro, sendo que somente estas
participarão da fase de lance (art. 24 do Decreto Estadual n.º 2.069/2006).

8 – DA FORMULAÇÃO DOS LANCES
8.1 Classificadas as propostas, o Pregoeiro dará início à fase competitiva, quando então os licitantes poderão encaminhar lances exclusivamente por meio do sistema eletrônico, sendo o licitante imediatamente informado do seu recebimento e respectivo horário de registro e valor.
8.1.1 Propostas cadastradas com valor mensal serão **excluídas** do certame por descumprimento dos termos do edital.
8.2 Os licitantes poderão oferecer lances sucessivos, observados o horário fixado e as regras de aceitação dos mesmos.
8.3 Somente serão aceitos os lances cujos valores forem inferiores ao último lance ofertado e registrado no sistema.
8.4 Não serão aceitos dois ou mais lances de mesmo valor, prevalecendo aquele que for recebido e registrado em primeiro lugar.
8.5 Durante o transcurso da sessão pública, os licitantes serão informados, em tempo real, do valor do menor lance registrado que tenha sido apresentado pelos demais licitantes, vedada à identificação do detentor do lance.
8.6 O encerramento da sessão pública dar-se-á por decisão do Pregoeiro, mediante encaminhamento de aviso de fechamento iminente dos lances, e, após o transcurso do prazo, determinado pelo sistema eletrônico, de até 30 (trinta) minutos, estará encerrada a recepção de lances.

8.7 No caso de desconexão do Pregoeiro, no decorrer da etapa de lances, se o sistema eletrônico permanecer acessível aos licitantes, os lances continuarão sendo recebidos, sem prejuízo dos atos realizados.
8.7.1 Quando a desconexão persistir por tempo superior a 10 (dez) minutos, a sessão do Pregão Eletrônico será suspensa e terá reinício somente após a comunicação expressa do Pregoeiro aos participantes.
8.8 A licitante será responsável por todas as transações que forem efetuadas em seu nome no Sistema Eletrônico, assumindo como firmes e verdadeiras sua proposta e lances (inciso III, art. 13º do Decreto n.º 5.450, de 2005).
8.9 Incumbirá ao licitante acompanhar as operações no Sistema Eletrônico durante a sessão pública do Pregão, ficando responsável pelo ônus decorrente da perda de negócios diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão (inciso IV, art. 13ºdo Decreto n.º 5.450, de 2005).
8.9.1 Sob pena de Desclassificação, o licitante deverá estar conectado e acompanhando a sessão pública. Será concedido o prazo de 20 (vinte) minutos para que ele se manifeste por meio do chat em resposta a qualquer indagação da Pregoeira. Se esgotado o referido prazo e o licitante não se manifestar, terá sua proposta desclassificada e a negociação encerrada, com fundamento no disposto no art. 14, inciso IV do Decreto Estadual n.º 2.069/2006.
8.10 Os preços propostos serão de exclusiva responsabilidade da licitante, não lhe assistindo o direito de pleitear qualquer alteração dos mesmos, sob alegação de erro, omissão ou qualquer outro pretexto.
8.11 A desistência injustificada do lance ofertado ou, ainda que justificada, não aceita pela pregoeira, implicará na inclusão respectiva ocorrência junto ao SICAF, sem prejuízo das demais sanções previstas na Lei e no edital.

9 – DO DIREITO DE PREFERÊNCIA DAS ME/EPP E EQUIPARADOS

9.1 Todos os licitantes deverão permanecer conectados até que o Pregoeiro possa verificar a ocorrência de um possível empate, pois, caso aconteça, serão tomadas as seguintes providências:
OBS.: Não poderão se beneficiar do regime diferenciado e favorecido em licitações, concedido às microempresas e empresas de pequeno porte, pela Lei Complementar n.º 123/06, que se enquadrem em qualquer das exclusões relacionadas no parágrafo quarto do seu artigo terceiro.
9.1.1 A ME/EPP ou equiparado considerado empatado e mais bem classificado deverá ser convocado, após o término dos lances, para apresentar nova proposta de preço inferior àquela considerada vencedora do certame em até 05 (cinco) minutos da convocação, sob pena de preclusão (Art. 45, inciso I c/c § 3º, da LC n.º 123/06);
9.1.2 A ME/EPP ou equiparado acima indicado que efetivamente apresente nova proposta de preço inferior àquela considerada vencedora do certame, desde que em tempo hábil, e atenda as demais exigências previstas neste Edital, terá adjudicado em seu favor o objeto licitado (Art. 45, I, da LC n.º 123/06);
9.1.3 Não ocorrendo contratação de ME/EPP ou equiparado na forma do subitem anterior, serão convocadas as ME/EPP e equiparados remanescentes considerados empatados na ordem classificatória para o exercício do direito de ofertar proposta de preço inferior àquela considerada vencedora do certame (Art. 45, II, da LC n.º 123/06).

9.2 Entende-se por empate aquelas situações em que as propostas apresentadas pelas ME/EPP e equiparados sejam iguais ou até 5% (cinco por cento) superiores ao lance mais vantajoso (Art. 44, §§ 1º e 2º, da LC n.º 123/06).
9.3 O critério de empate (5%) deverá ser aferido segundo o preço obtido **antes da negociação**.
9.4 No caso de equivalência dos valores apresentados pelas ME/EPP e equiparados que se encontrem em situação de empate, será realizado sorteio para que se identifique a primeira que poderá apresentar melhor oferta.
9.5 Somente se a contratação de ME/EPP ou equiparado que esteja dentro do critério de empate falhar é que o objeto licitado será adjudicado em favor da proposta originalmente vencedora, atendidas as demais disposições deste Edital (§ 1º do art. 45 da LC n.º 123/06).
9.6 O disposto neste item somente será aplicável quando a melhor oferta inicial não tiver sido apresentada por ME/EPP ou equiparado (Art. 45, § 3º, da LC n.º 123/06).

10 – DAS REGRAS GERAIS DE DESEMPATE
10.1 Se depois de realizado o procedimento previsto no item 09 "**DO DIREITO DE PREFERÊNCIA DAS ME/EPP E EQUIPARADOS**", restarem duas ou mais propostas em igualdade de condições, como critério de desempate, será assegurada preferência:
10.1.1 Sucessivamente, aos bens:
a) Produzidos no País;
b) Produzidos ou prestados por empresas brasileiras;
c) Produzidos ou prestados por empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País.
10.2 Na ausência das hipóteses de preferência acima enumeradas ou no caso de concurso entre as hipóteses previstas, a classificação far-se-á, obrigatoriamente, por sorteio, em ato público, para o qual todos os licitantes serão convocados, vedado qualquer outro processo.

11 – DA NEGOCIAÇÃO, ANÁLISE E DO JULGAMENTO DAS PROPOSTAS
11.1 Após o encerramento da etapa de lances, o Pregoeiro poderá encaminhar contraproposta diretamente ao licitante que tenha apresentado o lance mais vantajoso, para que seja obtida melhor proposta, observado o critério de julgamento e o valor estimado para a contratação, não se admitindo negociar condições diferentes das previstas neste Edital.
11.2 A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais licitantes.
11.3 O Pregoeiro poderá encaminhar, pelo sistema eletrônico, contraproposta, diretamente ao licitante que tenha apresentado a melhor oferta, para que seja obtido o desconto percentual mais vantajoso, bem como decidir sobre a sua aceitação, observado o critério de julgamento, não se admitindo negociar condições diferentes daquelas previstas no Edital (art. 25, § 8º do Decreto Estadual n.º 2.069/2006).
11.4 A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais licitantes.
11.5 O Pregoeiro examinará a proposta classificada em primeiro lugar quanto à compatibilidade do preço do objeto em relação ao estimado para a contratação.
11.6 Não poderá haver desistência dos lances ofertados, sujeitando-se o proponente desistente às penalidades constantes no item 23 deste Edital.

11.7 A classificação final far-se-á pela ordem crescente dos preços.
11.7.1 Será considerada mais vantajosa para a IOE a oferta de **MENOR PREÇO GLOBAL**, respeitados os limites máximos do preço unitário, na forma do item 6.10.2.
11.7.2 As propostas de preços deverão atender aos critérios de aceitabilidade de **MENOR PREÇO GLOBAL.** Propostas contendo preços com valores unitários acima do estimado para contratação serão negociadas pelo pregoeiro e, caso a licitante não aceite a negociação, a proposta será desclassificada.
11.7.3 A proposta deve apresentar preços unitários e totais, expressos em R$ (reais), com duas casas decimais, tanto em algarismos como por extenso. Em caso de divergência entre os preços unitários e totais, prevalecerão os primeiros, ocorrendo discordância entre os valores numéricos e por extenso, prevalecerão os últimos.
11.7.4 A proposta de preços ajustada ao lance final deve conter o valor (numérico e por extenso) dos preços unitários e totais, em valor líquido em moeda corrente nacional, com aproximação de até duas casas decimais, não podendo exceder o valor do lance final.
11.8 Aceita a proposta de **MENOR PREÇO GLOBAL**, será analisada a habilitação do licitante, para verificação do atendimento das condições fixadas no item 12 deste Edital.
11.9 Constatado o atendimento pleno às exigências editalícias, será declarado o proponente vencedor, sendo-lhe adjudicado o respectivo objeto, pelo Pregoeiro, caso não haja interposição de recursos.
11.10 Se a oferta não for aceitável ou se o proponente não atender às exigências editalícias, o Pregoeiro examinará as ofertas subsequentes, na ordem de classificação, até a apuração de uma proposta que atenda todas as exigências, sendo o respectivo proponente declarado vencedor e a ele adjudicado o objeto correspondente a sua proposta.
11.11 Na hipótese do item anterior, o Pregoeiro poderá negociar diretamente com o proponente para que seja obtido melhor preço.
11.12 Da reunião lavrar-se-á ata circunstanciada, na qual serão registradas as ocorrências relevantes e que, ao final, será assinada pelo Pregoeiro. Ressaltando-se que poderá constar a assinatura da equipe de apoio, sendo-lhes facultado este direito.
11.13 Será declarado vencedor, o licitante que apresentar proposta de acordo com as especificações do Edital e ofertar o **MENOR PREÇO GLOBAL** para o respectivo fornecimento do objeto.
11.14 O licitante declarado vencedor se obriga a adequar sua Proposta de Preços ao valor ofertado em seu lance e enviá-la, juntamente com a Documentação de Habilitação, no prazo de 48 (quarenta e oito) horas, via SEDEX ou outro meio igualmente idôneo, refazendo seus cálculos em função dos novos preços de forma que os valores assim calculados correspondam ao valor a ser efetivamente praticado.
11.15 O licitante vencedor se responsabiliza pelo valor de seu lance para a totalidade dos serviços licitados, não sendo aceito, em hipótese alguma, alegações de erros nos quantitativos, sob pena das cominações legais.

12 – DOS DOCUMENTOS DE HABILITAÇÃO

12.1 A habilitação do licitante que apresentar a melhor proposta será verificada *on line* no SICAF, na forma da legislação vigente, mediante análise dos documentos abrangidos pelo citado sistema.
12.1.1 Nos termos da Lei Federal n.º 12.440, de 07 de julho de 2011, a comprovação de inexistência de débitos inadimplidos perante a Justiça do Trabalho será aferida por meio da apresentação pelo licitante da

Certidão Negativa de Débitos Trabalhistas – CNDT, sem prejuízo da consulta pela Pregoeira ao sítio oficial de emissão.

12.1.2 Os documentos devem ser apresentados em nome do licitante e, preferencialmente, com número do CNPJ e endereço respectivo, observado o seguinte:

• se o licitante for a matriz da empresa, todos os documentos devem estar em nome da matriz;

• se o licitante for filial, todos os documentos devem estar em nome da filial;

- No caso de filial, é dispensada a apresentação dos documentos que, pela própria natureza, comprovadamente sejam emitidos somente em nome da matriz.

12.1.3 A proposta de preços e documentação de habilitação completa da empresa que teve o menor lance, deverão ser enviadas, em no máximo **60 (sessenta)** minutos, contados a partir da solicitação da Pregoeira para o **Sistema Eletrônico do COMPRASNET**, **exclusivamente, pelo "anexo"**, com o preço atualizado em conformidade com o lance ofertado, para substanciar as decisões na fase de aceitação.

12.1.4 O licitante vencedor, uma vez convocado deverá encaminhar à Imprensa Oficial do Estado, **via SEDEX ou outro meio igualmente idôneo no caso de ser declarado vencedor,** no **prazo de 48 (quarenta e oito) horas**, contados do final da sessão pública, os originais ou cópias autenticadas por meio de cartório competente, da documentação de habilitação, bem como o original da proposta de preços, devidamente assinada pelo representante legal, ajustada ao valor do lance dado ou negociado, observadas as exigências previstas neste edital e seus anexos, para o seguinte endereço:

Imprensa Oficial do Estado – IOE

Aos Cuidados do Setor de Licitações - Travessa do Chaco, n.° 2271, Bairro: Marco, CEP: 66.093-542 – Belém- Pará - Ref: Pregão Eletrônico n.º 010/2017

12.1.5. A não observância ao prazo estipulado no item 12.1.4, poderá ensejar, a critério da Pregoeira/ Administração, a recusa da proposta da licitante.

12.1.6. Não será permitido o envio de proposta de preços por outros meios eletrônicos que não seja o sistema COMPRASNET, sob pena da não aceitação da proposta e anexos implicando em desclassificação do licitante.

12.1.7. A PROPOSTA DE PREÇOS ENVIADA VIA SISTEMA COMPRASNET DEVERÁ CONTER:

a) Número do pregão, data e horário de abertura;

b) Razão social e CNPJ da empresa, endereço completo, telefone, fax e endereço eletrônico (e-mail), este último se houver, para contato, bem como nome do proponente ou de seu representante legal, CPF, RG e cargo na empresa, banco, agência, número da conta corrente e praça de pagamento;

c) Prazo de validade, não inferior a 60 (sessenta) dias corridos, a contar da data de sua abertura;

d) Especificações dos serviços de forma clara, descrevendo detalhadamente as características de todos os itens ofertados, que de forma inequívoca identifiquem e constatem as especificações cotadas;

e) Preço mensal e total do objeto de acordo com os lances ofertados, em algarismo e por extenso, expresso em moeda corrente nacional (R$), com no máximo 02 (duas) casas decimais, considerando as quantidades constantes no Termo de Referência - Anexo II do presente edital;

f) Declaração expressa de que nos preços cotados estão incluídas todas as despesas diretas e indiretas, frete, tributos, taxa de administração, encargos sociais, trabalhistas, transporte e seguro até o destino,

lucro e demais encargos de qualquer natureza necessários ao cumprimento integral do objeto deste Edital e seus anexos, nada mais sendo válido pleitear a esse título;
g) Declaração de garantia de que os Serviços serão substituídos, sem ônus para o Estado, caso não estejam de acordo com as especificações e padrões de qualidade exigidos.

12.2 Declarações:

12.2.1 Declaração do licitante, por meio do sistema eletrônico no momento de lançamento da proposta, de Inexistência e Fato Impeditivo da Habilitação e de Compromisso de Comunicação de sua eventual superveniência;
12.2.2 Declaração do licitante, por meio do sistema eletrônico no momento de lançamento da proposta, de que não possui em seu quadro de pessoal empregado(s) menor (es) de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre e de 16 (dezesseis) anos em qualquer trabalho, salvo na condição de aprendiz, a partir de 14 (quatorze) anos, nos termo do inciso XXXIII, do art. 7º, da CF/88;
12.2.3 Declaração do licitante, por meio do sistema eletrônico no momento de lançamento da proposta, de elaboração independente de proposta (Portaria n.º51, de 03 de julho de 2009, da Secretaria de Direito Econômico, órgão vinculado ao Ministério da Justiça e Instrução Normativa n.º 02, de 16.09.2009, publicada no D.O.U n.º 178, Seção I, pág. 80, de 17.09.2009);
12.2.4 Declaração de que conhece as condições para execução dos serviços objeto desta licitação, nada podendo alegar em seu favor futuramente caso seja a vencedora do certame.

12.3 Para Habilitação Jurídica:

12.3.1 Registro comercial, no caso de empresa individual;
12.3.2 Ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado, em se tratando de sociedades comerciais. No caso de sociedades comerciais ou sociedades por ações, deverão ser acompanhados de documentos de eleição de seus administradores, no qual deverá estar contemplado, dentre os objetivos sociais, a execução de atividades da mesma natureza ou compatíveis com o objeto da licitação;
12.3.3 Inscrição do ato constitutivo no órgão competente, acompanhada, no caso de sociedades civis, de prova da diretoria em exercício;
12.3.4 A empresa estrangeira em funcionamento no país deverá apresentar também o Decreto de Autorização e o Ato de Registro ou Autorização para Funcionamento expedido pelo órgão competente, quando a atividade assim o exigir.

12.4 Para Regularidade Fiscal e Trabalhista:

12.4.1 Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas – CNPJ;
12.4.2 Prova de inscrição no Cadastro de Contribuintes Estadual e Municipal, se houver relativo ao domicilio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto deste edital.
12.4.3 Prova de regularidade com as fazendas públicas:
a) Federal: A prova de regularidade fiscal perante a Fazenda Nacional será efetuada mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil - RFB e pela Procuradoria-Geral da Fazenda Nacional - PGFN, referente a todos os tributos federais e à Dívida Ativa da União - DAU por elas administrados;
b) Estadual (se a sede da empresa for no Estado do Pará, a regularidade será comprovada por meio de duas certidões: tributária e não tributária); e

c) Municipal (se a sede da empresa for no município de Belém, a regularidade será comprovada por meio de uma única certidão, em conformidade com o disposto na Instrução Normativa n.º 06/2009 – GABS/SEFIN).

12.4.4 Prova de Regularidade com Fundo de Garantia por Tempo de Serviço – FGTS;

12.4.5 Prova de Regularidade Trabalhista perante a Justiça do Trabalho, através da apresentação da Certidão Negativa de Débitos Trabalhistas, conforme Lei n.º 12.440, de 07 de julho de 2011.

12.5 Para Qualificação Técnica:

12.5.1 Apresentar pelo menos 01 (um) Atestado de Capacidade Técnica, fornecido por pessoa jurídica de direito público ou privado (conforme Lei 8.666/93, Art. 30, Inciso II, Parágrafo 1º), a fim de comprovar que a empresa licitante/vencedora desempenhou ou desempenha atividade pertinente e compatível em características e quantidades com o objeto da licitação.

12.5.2 O atestado de capacidade técnica deve ser emitido em nome e com CNPJ/MF da matriz e/ou da(s) filial (ais) da licitante proponente responsável pela execução do serviço ou entrega do objeto.

12.5.3 Os atestados de capacidade técnico-operacional deverão referir-se a serviços prestados no âmbito de sua atividade econômica principal ou secundária especificadas no contrato social vigente;

12.5.4 Somente serão aceitos atestados expedidos após a conclusão do contrato ou se decorrido, pelo menos, um ano do início de sua execução, exceto se firmado para ser executado em prazo inferior.

12.5.5 O licitante deve disponibilizar quando solicitado, todas as informações necessárias à comprovação da legitimidade dos atestados solicitados, apresentando, dentre outros documentos, cópia do contrato que deu suporte à contratação, endereço atual da **CONTRATANTE** e local em que foram prestados os serviços.

12.5.6 Comprovação de que tenha executado serviços compatíveis em quantidade com o objeto licitado por período não inferior a 12 (doze) meses;

12.5.7 Para a comprovação da experiência mínima de 12 (doze) meses prevista neste subitem, será aceito o somatório de atestados.

12.5.8 Os Atestados de Capacidade Técnica deverão ser originais, admitida cópia autenticada.

12.6 Para Qualificação Econômico-Financeira:

12.6.1 Certidão negativa de falência, recuperação judicial, ou extrajudicial expedida pelo Cartório de Distribuição da sede do licitante, nos últimos 30 (trinta) dias que antecedem a abertura da licitação, quando o prazo de sua validade não estiver definido;

12.6.2 Balanço patrimonial e demonstrações contábeis do último exercício social, já exigível e apresentado na forma da lei, vedada sua substituição por balancetes ou balanços provisórios, podendo ser atualizados por índices oficiais quando encerrados há mais de 03 (três) meses da data de apresentação da proposta, que permitam aferir a condição financeira da empresa;

12.6.3 A comprovação de boa situação financeira da licitante será aferida com base nos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), todos maiores ou iguais a 1 (um), resultantes da aplicação das fórmulas abaixo, **evidenciadas pelo próprio licitante**:

LG = (Ativo Circulante + Realizável a Longo Prazo) : (Passivo Circulante + Exigível a Longo Prazo)

SG = Ativo Total : (Passivo Circulante + Exigível a Longo Prazo)

LC = Ativo Circulante : Passivo Circulante

12.6.3.1 As empresas que apresentarem resultado inferior ou igual a 01 (um) em qualquer dos índices referidos no subitem anterior deverão comprovar o capital mínimo ou valor do patrimônio líquido de 10% do valor estimado da contratação, devendo a comprovação ser feita relativamente à data da apresentação da proposta de preços, na forma da lei, de acordo com os §§ 2º e 3º do artigo 31 da Lei n.º 8666/93.
12.7 Os proponentes, devidamente atualizados no SICAF, ficam dispensados da apresentação dos documentos descritos nos subitens, **12.4.1**, **12.4.2**, **12.4.3, 12.4.4, 12.4.5 e 12.6.2**, sendo consultada *on line* a respectiva regularidade do proponente junto àquele cadastro.
12.8 Os documentos necessários à habilitação deverão ser apresentados em original, ou em cópia autenticada em Cartório competente, ou publicação em órgão da imprensa oficial ou em cópias simples, desde que acompanhados dos originais, enviados a Pregoeira para conferência.
12.8.1 Em se tratando de microempresa ou empresa de pequeno porte, havendo alguma restrição na comprovação da regularidade fiscal e/ou trabalhista, será assegurado o prazo de 05 (cinco) dias úteis, cujo termo inicial corresponderá ao momento em que a proponente for declarada vencedora do certame, prorrogável por igual período, a critério da Administração, para regularização da documentação, pagamento ou parcelamento do débito, e emissão de eventuais certidões negativas ou positivas com efeito de certidão negativa;
12.9 O invólucro contendo a documentação deve ser endereçado para:

IMPRENSA OFICIAL DO ESTADO – IOE
LICITAÇÕES/IOE
PREGÃO ELETRÔNICO N.º 010/2017/IOE
ENDEREÇO: TRAVESSA DO CHACO, N.º 2271
BAIRRO: MARCO, CEP: 66.093-542 BELÉM-PA

12.10 Para fins de habilitação, a verificação em sítios oficiais de órgãos e entidades emissores de certidões constitui meio legal de prova.
12.11 À Pregoeira ou à Autoridade Superior é assegurado o direito de solicitar ao licitante vencedor, a qualquer tempo, no curso da licitação, quaisquer esclarecimentos sobre os documentos já entregues, fixando-lhes prazo para atendimento.
12.12 Disposições gerais da habilitação:
12.12.1 Não serão aceitos protocolos de entrega ou solicitação de documento em substituição aos documentos requeridos no presente Edital e seus anexos;
12.12.2 Se a documentação de habilitação não estiver completa e correta ou contrariar qualquer dispositivo deste Edital e seus anexos, a Pregoeira considerará o proponente inabilitado.
12.13 Quando todos os licitantes foram inabilitados, a Pregoeira poderá, obedecida a ordem de classificação das propostas, fixar-lhes o prazo de 8 (oito) dias úteis para a apresentação de novos documentos.
12.13.1 Serão aceitas somente cópias legíveis, respeitando o item 12.8;
12.13.2 Não serão aceitos documentos cujas datas estejam rasuradas;

12.13.3 À Pregoeira reserva-se o direito de solicitar o original de qualquer documento, sempre que tiver dúvida ou julgar necessário.
12.14 Os documentos a serem protocolados deverão ser apresentados, preferencialmente, grampeados e/ou encadernados, na ordem mencionada.

13 – DOS RECURSOS
13.1 É admissível a interposição de recurso compreendida a manifestação prévia do licitante, durante a sessão pública, realizada exclusivamente no âmbito do sistema eletrônico.
13.2 Existindo intenção de interpor recurso, o licitante deverá manifestá-la ao Pregoeiro, por meio eletrônico, explicando sucintamente suas razões, imediatamente após a divulgação do vencedor.
13.3 O licitante dispõe do prazo de 3 (três) dias úteis para a apresentação do recurso, por escrito, que ficará disponível a todos os participantes, tão logo seja encaminhado ao Pregoeiro.
13.3.1 Os demais licitantes poderão apresentar contrarrazões em até 3 (três) dias úteis, contados a partir do término do prazo recorrente.
13.4 Os recursos e as contrarrazões deverão ser disponibilizados pelos licitantes no sítio *www.comprasnet.gov.br***.**
13.5 É assegurada aos licitantes vista imediata dos atos do Pregão Eletrônico, com a finalidade de subsidiar a preparação de recursos e de contrarrazões, observados os prazos da legislação pertinente.
13.6 A decisão do Pregoeiro deverá ser motivada.
13.6.1 À autoridade competente cabe decidir os recursos contra os atos do Pregoeiro, quando este mantiver sua decisão (art. 9º, inciso III do Decreto Estadual n.º 2.069/2006).
13.7 A falta de manifestação imediata e motivada do licitante importará na decadência do direito de recurso e na adjudicação do objeto pelo Pregoeiro ao vencedor.
13.8 O acolhimento do recurso importará na invalidação apenas dos atos insuscetíveis de aproveitamento.
13.8.1 Não serão conhecidos recursos interpostos após os respectivos prazos legais.
13.9 Os recursos e as contrarrazões que forem envidados por FAC-SÍMILE, deverão ter seus originais encaminhados em até 5 (cinco) dias úteis após o prazo recursal.
13.10 Os autos do processo permanecerão com vista franqueada aos interessados junto ao Pregoeiro da autarquia.
13.11 As razões dos recursos deverão ser apresentadas por escrito, protocoladas tempestivamente na sede da IOE, localizada na Travessa do Chaco, n.º 2271, bairro: Marco, Belém-PA – CEP: 66.093-542, e dirigidas à Autoridade Superior, a qual decidirá sobre os recursos após apreciação do parecer do Pregoeiro.
13.12 Qualquer recurso ou impugnação contra a decisão do Pregoeiro não terá efeito suspensivo e, se acolhido invalidará apenas os atos insuscetíveis de aproveitamento.

14 – DA ADJUDICAÇÃO
14.1 O objeto deste Pregão Eletrônico será adjudicado pelo Pregoeiro, se não houver interposição de recursos, depois de atendidas as condições deste Edital, cuja homologação caberá ao Presidente da IOE.

14.2 Se houver interposição de recurso e caso seja mantida a decisão pelo Pregoeiro, caberá a Autoridade Superior a análise do recurso, bem como a adjudicação do objeto ao licitante vencedor e a homologação do certame, conforme art. 28 do Decreto Estadual n.º 2.069/2006.

15 – DA CONTRATAÇÃO

15.1 A contratação será formalizada através de instrumento de Contrato ou outro instrumento hábil, na forma do art. 62 da Lei de Licitações.

15.2 A IOE convocará o vencedor da licitação, que terá o prazo de até 05 (cinco) dias úteis, para assinar o instrumento de contrato ou receber a nota de empenho, sob pena de decair do direito à contratação, sem prejuízo das sanções previstas no art. 81 da Lei n.º 8.666/93.

15.3 Na assinatura do contrato será exigida a comprovação das condições de habilitação consignadas no Edital, e, quando o proponente vencedor não apresentar situação regular ou recusar-se a assiná-lo, injustificadamente, será convocado outro licitante, observada a ordem de classificação, para celebrar o contrato, e assim sucessivamente, sem prejuízo da aplicação das sanções cabíveis.

154 É vedada a prorrogação do contrato quando:

15.4.1 Os preços estiverem superiores aos estabelecidos como limites por meio de atos normativos do Governo do Estado do Pará, admitindo-se a negociação para redução de preços;

15.4.2 A **CONTRATADA** tiver sido declarada inidônea ou suspensa no âmbito do Estado ou da própria entidade contratante, enquanto perdurarem os efeitos.

15.4.3 A **CONTRATADA** não mantiver as condições de habilitação e qualificação exigidas na licitação.

15.5 No ato da contratação será exigida, ainda, Declaração do licitante de que possui em seu quadro de empregados um percentual mínimo de 5% (cinco por cento) de pessoas com deficiência, nos termos do § 6º do art. 28 da Constitucional Estadual, conforme modelo do Anexo I, n.º 1;

15.5.1 As empresas que possuírem no seu quadro funcional menos de 20 (vinte) empregados ficam dispensadas do cumprimento da exigência acima, devendo, nesse caso, apresentar a declaração constante do Anexo I, n.º 2.

16 – DA FISCALIZAÇÃO

16.1 A fiscalização da contratação será exercida por um representante da Administração, ao qual competirá dirimir as dúvidas que surgirem no curso da execução do contrato, e de tudo dará ciência à Administração.

16.2 O acompanhamento e a fiscalização da execução do contrato consistem na verificação da conformidade do fornecimento dos produtos, execução dos serviços e da alocação dos recursos necessários, de forma a assegurar o perfeito cumprimento do contrato, e será exercido por servidor especialmente designado para esse fim atuando como Fiscal do Contrato, pela Imprensa Oficial do Estado - IOE, **na forma art. 67 da Lei n.º 8.666/93**, ficando a **CONTRATADA** obrigada a atender às observações de caráter técnico do fiscal, que se acha investido de plenos poderes para:

16.2.1 Conferir se o objeto está de acordo com as especificações técnicas exigidas;

16.2.2 Informar à Diretoria Administrativa e Financeira da IOE, as ocorrências que exijam decisões e providências que ultrapassem a sua competência.

16.3 O representante da **CONTRATANTE** deverá ter a experiência necessária para o acompanhamento e controle da execução do contrato.
16.4 A fiscalização de que trata este item não exclui nem reduz a responsabilidade da fornecedora, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, ou emprego de material inadequado ou de qualidade inferior, e, na ocorrência desta, não implica em corresponsabilidade da Administração ou de seus agentes e prepostos, de conformidade com o art. 70 da Lei n.º 8.666, de 1993.
16.5 O fiscal do contrato anotará em registro próprio todas as ocorrências relacionadas com a execução do contrato, indicando dia, mês e ano, bem como o nome dos funcionários eventualmente envolvidos, determinando o que for necessário à regularização das faltas ou defeitos observados e encaminhando os apontamentos à autoridade competente para as providências cabíveis.

17 – DAS CONDIÇÕES DE ENTREGA DO OBJETO
17.1 O prazo de entrega/disponibilização do objeto obedecerá ao disposto no Termo de Referência (ANEXO II).
18 – DO RECEBIMENTO PROVISÓRIO E DEFINITIVO
18.1 O objeto do presente certame será recebido de acordo com os prazos e condições previstos no Termo de Referência (ANEXO II).

19– DA RESPONSABILIDADE DA CONTRATADA
19.1 A**CONTRATADA** é responsável pelos danos causado à Administração ou a terceiros, decorrentes de sua culpa ou dolo na execução do contrato.
19.2 O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da **CONTRATADA** pelos prejuízos resultantes da incorreta execução do contrato.

20 – DA GARANTIA DO PRODUTO
20.1 O produto deverá possuir prazo de garantia mínima de 12 (doze) meses, contados a partir do da implantação do sistema.
20.2 Durante o prazo de garantia, a **CONTRATADA** obriga-se a substituir ou reparar, às suas expensas, qualquer produto que apresente defeito que não seja decorrente do desgaste natural ou do incorreto manuseio do produto.

21 – DO PAGAMENTO E DO REAJUSTE
21.1 Pela efetiva entrega e implantação do objeto, o pagamento será efetuado, mediante o processamento normal de liquidação, através da Diretoria Administrativa e Financeira da IOE, em até 30 (trinta) dias, mediante Ordem Bancária em conta corrente da CONTRATADA, em tudo obedecidos o Decreto Estadual n.º 877, de 31 de março de 2008 e Instrução Normativa n.º 0018, de 21 de maio de 2008 da Secretaria de Estado da fazenda – SEFA.
21.2 Pelos serviços de manutenção, o pagamento será efetuado, mensalmente, após a efetiva comprovação da execução dos serviços, mediante o processamento normal de liquidação, através da Diretoria Administrativa e Financeira da IOE, em até 30 (trinta) dias, mediante Ordem Bancária

em conta corrente da CONTRATADA, em tudo obedecidos o Decreto Estadual n.º 877, de 31 de março de 2008 e Instrução Normativa n.º 0018, de 21 de maio de 2008 da Secretaria de Estado da fazenda – SEFA.

21.3 Não haverá, sob hipótese alguma, pagamento antecipado à **CONTRATADA**.

21.4 Havendo erro na nota fiscal/fatura, ou circunstância que impeça a liquidação da despesa, aquela será devolvida à **CONTRATADA** e o pagamento ficará pendente até que seja sanado o problema ocorrido, o que deve ocorrer em até 30 (trinta) dias. Nesta hipótese, o prazo para pagamento se iniciará após a regularização da situação ou reapresentação do documento fiscal, não acarretando qualquer ônus para a **CONTRATANTE**.

21.5 O pagamento só será realizado após a comprovação da regularidade fiscal da **CONTRATADA**.

21.6 O preços dos serviços de manutenção contratados com prazo de vigência igual ou superior a doze meses será reajustado a cada interregno de 01 (um) ano, mediante a aplicação do índice setorial ou IGPM ou outro que venha substituí-lo.

21.7 O interregno mínimo de 01 (um) ano para o primeiro reajuste será contado a partir da data limite para apresentação das propostas constante do Edital.

21.8 Nos reajustes subsequentes ao primeiro, o interregno mínimo de 01 (um) ano será contado a partir da data de início da vigência do reajuste anterior.

22 – DAS SANÇÕES ADMINISTRATIVAS

22.1 Nos termos do art. 7º da Lei n.º 10.520, de 17 de julho de 2002, ficará impedida de licitar e contratar com a União, Estados, Distrito Federal e Municípios, pelo prazo de até 5 (cinco) anos, garantido o direito prévio do contraditório e da ampla defesa, sem prejuízo das sanções previstas no subitem 23.2, o licitante que:

22.1.1 Se recusar a assinar o contrato;

22.1.2 Ensejar o retardamento da execução do objeto deste Pregão Eletrônico;

22.1.3 Não mantiver a proposta, injustificadamente;

22.1.4 Comportar-se de modo inidôneo;

22.1.5 Fizer declaração falsa;

22.1.6 Cometer fraude fiscal;

22.1.7 Falhar ou fraudar na execução do objeto.

22.2 Pela inexecução total ou parcial do objeto deste Pregão Eletrônico, a IOE poderá, garantida a prévia defesa, aplicar à **CONTRATADA** as sanções fixadas a seguir, sem prejuízo de outras previstas em lei:

a) Advertência;

b) Multa de 1,0(um por cento) por dia de atraso incidente sobre o valor do faturamento, no todo ou em parte, e que será cobrado em dobro a partir do 31º (trigésimo primeiro) dia de atraso;

c) Multa de até 10% (dez por cento) sobre o valor total do Contrato, por infração de qualquer cláusula contratual, dobrável na reincidência;

d) Suspensão temporária de participar em licitação e impedimento de contratar com a Imprensa Oficial Estado, pelo prazo de até 02 (dois) anos;

e) 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.
f) A multa será aplicada sobre o valor do Contrato e será descontada dos pagamentos eventualmente devidos pela **CONTRATANTE** ou cobrada judicialmente.
g) As multas previstas neste Contrato são independentes entre si, podendo ser aplicadas isoladas ou cumulativamente.
h) O valor das multas aplicadas deverá ser recolhido em favor da **CONTRATANTE**, no prazo de 05 (cinco) dias, a contar da data da notificação, podendo a **CONTRATANTE**, descontar o seu valor das notas fiscais e/ou faturas por ocasião do seu pagamento, ou cobrá-las judicialmente, pelo processo de execução fiscal, com
os respectivos encargos, segundo a Lei n.º 6.830/80.
i) Caberá recurso do ato que aplicar a penalidade, no prazo de 05 (cinco) dias úteis, a contar da respectiva ciência, sem efeito suspensivo.
22.3 Comprovado impedimento ou reconhecida força maior, devidamente justificado e aceito pela IOE, o licitante e/ou **CONTRATADA** ficará isento (a) das penalidades mencionadas.
22.4 As penalidades serão obrigatoriamente registradas no **SICAF**, e no caso de suspensão de licitar, o licitante deverá ser descredenciado por igual período, sem prejuízo das multas previstas neste Edital e das demais cominações legais.
22.5 A desistência injustificada do lance ofertado ou, ainda que justificada, não aceita pelo pregoeiro e a não observância do prazo para assinatura do contrato, implicarão na inclusão da respectiva ocorrência junto ao SICAF, sem prejuízo das demais sanções previstas na Lei e no Edital:
a) Advertência – inciso I, art. 87 da Lei n.º 8.666/93;
b) Multa – art. 87, II da Lei n.º 8.666/93;
c) Suspensão Temporária – art. 87, III da Lei n.º 8.666/93;
d) Declaração de idoneidade – art. 87, IV da Lei n.º 8.666/93;
e) Impedimento de licitar e contratar com a administração pública – art. 7º da Lei n.º 10.520/02.

23 – DO PREGÃO ELETRÔNICO

24.3.1 A critério da IOE, este Pregão Eletrônico poderá:
23.1.1 Ser anulado se houver ilegalidade de ofício ou por provocação de terceiros, mediante parecer escrito e devidamente fundamentado;
23.1.2 Ser revogado, a juízo da IOE, se for considerado inoportuno ou inconveniente ao interesse público, decorrente de fato superveniente comprovado, pertinente e suficiente para justificar tal conduta;
23.1.3 Ter sua data de abertura da sessão pública transferida, por conveniência exclusiva da IOE.
23.2 Será observado, ainda, quando ao procedimento deste Pregão Eletrônico:
23.2.1 A anulação do procedimento licitatório por motivo de ilegalidade não gera obrigação de indenizar, ressalvado o disposto no parágrafo único do art. 59 da Lei n.º 8.666/93.
23.2.2 A nulidade do procedimento licitatório induz à da nota de empenho, ressalvado, ainda, o dispositivo citado no subitem anterior.

23.3 No caso de desfazimento do processo licitatório ficam assegurados o contraditório e a ampla defesa.

24 – DA IMPUGNAÇÃO DO ATO CONVOCATÓRIO E DA SOLICITAÇÃO DE ESCLARECIMENTOS

24.1 Até 02 (dois) dias úteis antes da data fixada para abertura da sessão pública, qualquer pessoa poderá impugnar o ato convocatório de PREGÃO ELETRÔNICO (art. 19 do Decreto Estadual n.º 2.069/2006).

24.1.1 Caberá ao Pregoeiro, auxiliado pelo setor responsável, decidir sobre a petição no prazo de 24 (vinte e quatro) horas;

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

24.2 A impugnação feita tempestivamente não impedirá o licitante de participar deste processo licitatório até o trânsito em julgado da decisão a ela pertinente.

24.3 Os pedidos de esclarecimentos referentes ao processo licitatório deverão ser enviados ao Pregoeiro, até 3 (três) dias úteis anteriores à data fixada para abertura da sessão pública, EXCLUSIVAMENTE POR MEIO
ELETRÔNICO VIA *INTERNET*, pelo *e-mail* *licitacao@ioe.pa.gov.br*.

25 – DAS DISPOSIÇÕES GERAIS

25.1 É facultado ao Pregoeiro ou à Autoridade Superior, em qualquer fase da licitação, promover diligência destinada a esclarecer ou complementar a instrução do processo.

25.2 Os proponentes assumem todos os custos de preparação e apresentação de suas propostas e a IOE não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do processo licitatório.

25.3 Os proponentes são responsáveis pela fidelidade e legitimidade das informações e dos documentos apresentados na licitação.

25.4 Após aberta a sessão, não caberá desistência dos lances ofertados, salvo por motivo justo decorrente de fato superveniente e aceito pelo Pregoeiro.

25.5 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, nos mesmos
horários e sítio estabelecidos, desde que não haja comunicação do Pregoeiro em contrário.

25.6 O desatendimento de exigências formais não essenciais não implicará o afastamento do licitante, desde que seja possível a aferição da sua qualificação e a exata compreensão da sua proposta, durante a realização da
sessão pública do Pregão Eletrônico.

25.7 A homologação do resultado desta licitação não atribui à empresa vencedora o direito de fornecer os serviços referentes ao respectivo objeto.

25.8 O licitante será responsável por todas as transações que forem efetuadas em seu nome no sistema eletrônico, assumindo como firmes e verdadeiras sua proposta e lances, inclusive os atos praticados diretamente ou por seu representante, não cabendo ao provedor do sistema ou à IOE, responsabilidade por

eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros(art. 14, inciso III do Decreto Estadual n.º 2.069/2006).
25.9 Incumbirá ao licitante acompanhar as operações no sistema eletrônico durante a sessão pública do Pregão Eletrônico, ficando responsável pelo ônus decorrente da perda de negócios diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão (art. 14, inciso IV do Decreto Estadual n.º 2.069/2006).
25.10 As normas que disciplinam este Pregão Eletrônico serão sempre interpretadas em favor da ampliação da disputa entre os interessados, sem comprometimento do interesse da Administração, a finalidade e a segurança da contratação.
25.11 Para todas as referências de tempo contidas neste edital será observado o **horário de Brasília (DF).**

26 – DOS ANEXOS DO EDITAL
26.1 Constituem Anexos deste Edital os seguintes documentos:
26.1.1 ANEXO I – Modelo de Declaração de Cumprimento do §6º art. 28 da Constituição do Estado do Pará (Declaração de empregabilidade de pessoa com deficiência);
26.1.2 ANEXO II – Termo de Referência;
26.1.2.1 – Apêndice I do ANEXO II (Termo de Referência) – Modelo de Declaração de Vistoria;
26.1.3 ANEXO III – Modelo de Proposta de Preço;
27.1.4 ANEXO IV – Minuta de contrato.

Belém (PA), 08 de maio de 2017.

JANETE BARRETO
PREGOEIRA

ANEXO I DO PREGÃO ELETRÔNICO N.º 010/2017/IOE
(APRESENTAR DECLARAÇÃO NO ATO DA CONTRATAÇÃO)
Modelo n.º 01

MODELO DE DECLARAÇÃO DE CUMPRIMENTO D0 §6º ART. 28 DA CONSTITUIÇÃO DO ESTADO DO PARÁ (DECLARAÇÃO QUE EMPREGA 5% DE PESSOAS COM DEFICIÊNCIA)

(Nome da empresa) _____, CNPJ n.º _____, estabelecida a _____ (endereço completo), por intermédio de seu representante legal, o (a) Sr. (a) _____, portador (a) da carteira de Identidade n.º _____ e do CPF n.º _____, declara, para fim do disposto no Inciso I do Art. 27 da Lei n.º 8.666 de 21 de junho de 1993, que possui em seu quadro de pessoal, 5% (cinco por cento) de pessoas com deficiência em atendimento ao disposto no § 6º do art. 28 da Constituição do Estado do Pará.

Cidade (UF), _____ de _____ de 2017.

_____
Assinatura e carimbo do representante

Modelo n.º 02

MODELO DE DECLARAÇÃO DE NÃO EMPREGABILIDADE DE DEFICIENTES

(Nome da empresa) _____, CNPJ n.º _____, estabelecida a _____ (endereço completo), por intermédio de seu representante legal, o (a) Sr. (a) _____, portador (a) da carteira de Identidade n.º _____ e do CPF n.º _____, declara, para fim do disposto no Inciso I do Art. 27 da Lei n.º 8.666 de 21 de junho de 1993, que **não** possui em seu quadro de pessoal, 5% (cinco por cento) de pessoas com deficiência em atendimento ao disposto no § 6º do art. 28 da Constituição do Estado do Pará (EC nº 0042/2008, publicada em 11.06.2008), **em função de possuir menos de 20 (vinte) funcionários em seu quadro de pessoal.**

Cidade (UF), _____ de _____ de 2017.

_____
Assinatura e carimbo do representante

ANEXO II DO PREGÃO ELETRÔNICO N.º 010/2017/IOE
SERVIÇOS DE SEGURANÇA DIGITAL - TERMO DE REFERÊNCIA

DESCRITIVO TÉCNICO – SOLUÇÃO AVANÇADA DE PROTEÇÃO DE ATIVOS DE TECNOLOGIA

1.1. Objeto: Aquisição de serviços de segurança da informação, fornecendo e integrando firewalls UTM, firewalls de aplicação WEB, gestão de senhas de alto-privilégio e proteção contra ameaças avançadas (ANTI-RANSOMWARE), incluindo filtro de pacote, administração de largura de banda (QoS), VPN, IPSec, SSL e IPS, antivírus, anti-spyware, para atendimento às características técnicas mínimas descritas, contemplando o fornecimento de hardwares, softwares e solução em nuvem, bem como serviços de instalação, configuração, suporte, avaliação de ambientes, monitoramento contínuo, repasse tecnológico e migração das regras de firewall atualmente implementadas para as novas soluções.

1.2. Objetivo

Com o crescimento dos ataques e espionagem virtual aos quais os órgãos governamentais e empresas privadas têm sido vítimas, torna-se extremamente necessária a utilização de recursos que auxiliem, de forma proativa, a prevenção das vulnerabilidades encontradas em diversos vetores – redes (perímetro), sistemas de mensagens eletrônicas (e-mail), firewalls específicos para aplicações web e senhas de alto privilégio e endpoint (estações de trabalho do usuário).

A IOE possui um ativo extremamente valioso e do qual sua proteção é imprescindível: A INFORMAÇÃO, especialmente a que abrange os documentos recebidos para publicação no Diário Oficial do Estado, e os próprios arquivos digitais do jornal. O órgão trata um grande volume de informações e processos e precisa garantir confidencialidade, disponibilidade e integridade destas informações. Para que seja atendido esse nível de segurança, exigido nos dias atuais, é necessário investir em sistemas e conhecimento específicos contra ameaças avançadas e especificamente direcionadas para as quais ainda não exista uma “vacina”. Além disso, é igualmente imprescindível que seja realizada de forma segura a gestão das senhas de alto privilégio de ativos e sistemas. O resultado esperado é evitar que sejamos vítimas de organizações especializadas na execução de crimes virtuais.

A maioria das ameaças utiliza vulnerabilidades existentes em aplicações, na rede ou anexos de e-mail para os funcionários. Esse último é conhecido como Phishing e atualmente é o maior vetor de

ataque, pois se baseia na inexperiência dos funcionários. Por isso, é necessária a aquisição de um serviço que possa, de forma customizada ao ambiente, interceptar e inutilizar tais ameaças.

O ransomware é um tipo de malware que sequestra o computador da vítima e cobra um valor em dinheiro pelo resgate, geralmente usando a moeda virtual bitcoin, que torna quase impossível rastrear o criminoso que pode vir a receber o valor. Este tipo de ataque age codificando os dados do sistema operacional de forma com que os usuários não tenham mais acesso.

Sites governamentais estão sempre na mira de criminosos cibernéticos e o Brasil, segundo uma pesquisa, é o país com maior número de sites governamentais com a segurança comprometida. Em 2014, relatório do Gabinete de Segurança Institucional da República apontou que foram registradas 400 invasões em computadores do governo federal, que resultaram em vazamento de informação sensível. Não foi divulgado se houve pedido de resgate para devolução dos dados.

Para os governos, além do perigo de vazamento de dados sensíveis, existe a preocupação de que a população perca a confiança nos serviços virtuais, entre outras inúmeras consequências.

Todo mês, são acessados milhões de sites infectados por ransomware e, caso não existam soluções de segurança capazes de bloquear os ataques, evitando o impacto do ransomware, o risco de ser alvo dos criminosos e ter seus dados “sequestrados” é alto.

1.3. Lista de Preocupações

A grande parte das violações a dados sensíveis ocorrem quando os controles básicos são ineficazes ou inexistentes. Se debilidades evidentes ficam expostas, as chances são de que um atacante irá explorá-las. Como uma extensão específica a isso, não podemos negligenciar que os criminosos virtuais ganhem acesso aos dados sensíveis das organizações também através do compartilhamento das redes, ou mesmo com uso de credenciais roubadas ou compartilhadas.

Mas, outras linhas de defesa devem passar a fazer parte do universo disponível aos administradores de segurança: o monitoramento dos acessos, verificação do tipo de tráfego e verificação do comportamento do tráfego em tempo real, identificando acessos abusivos ou indevidos.

Qualquer que seja a sofisticação e agressividade dos ataques, a capacidade de detectar uma violação quando ela está ocorrendo é um enorme obstáculo para a maioria das organizações. Se a deficiência está na tecnologia ou no processo o fato é que poucas vítimas conseguem descobrir suas violações e, menos ainda, descobri-las em tempo hábil. Como desafios, podemos listar a necessidade de assegurar que os controles essenciais estão preenchidos, pesquisando, acompanhando e avaliando os dados; coletar e monitorar logs de evento; auditar contas de usuário e suas credenciais; promover a identificação da origem e o destino pretendido dos acessos.

Integram, também, a lista de preocupações os seguintes ítens:

- As senhas de alto privilégio e controle das aplicações são um fator critico para o gerenciamento do ambiente;
- O ambiente de ameaças se altera rapidamente e um número grande e crescente das chamadas "ameaças web", em um número infinito de variantes, estão causando estragos, geralmente, sem o conhecimento das secretarias, órgãos e empresas afetadas.
- O ambiente de ameaças cresce rapidamente e ataques em grande volume com objetivo de constranger a infraestrutura e gerar indisponibilidade nas aplicações são cada vez mais frequentes;
- Os criminosos virtuais estão roubando desde listas de números de CPF de empresas de planos de saúde, números de cartão de crédito de instituições financeiras a informações confidenciais de empresas de tecnologia e recursos de todos os setores privados e governamentais;
- As ameaças mistas geram comprometimento em massa e os ataques direcionados por meio de novos emergentes métodos; incluindo técnicas avançadas de engenharia social;
- A técnica de acessos anônimos, onde usuários conseguem burlar as regras de bloqueio com utilização de aplicativos nas estações de trabalho;
- Multiplicarem-se os vírus, worms e cavalos de Tróia;
- As técnicas inovadoras dos criminosos virtuais;
- As técnicas de exibição de conteúdo de propaganda como anúncio de pop-up;
- As técnicas de coleta de informações demográficas e de usuários são recolhidas e enviadas para um servidor remoto pela Internet (Call back);
- Plug-ins de ajuda do navegador que podem monitorar ou manipular a navegação do usuário na web.
- Crime eletrônico como ferramentas de hacker que são usadas como componentes de frauds inovadoras;
- Ferramentas de hacker que são programas projetados para romper medidas de segurança de computadores e de redes

2. JUSTIFICATIVA

2.1. Preservar a integridade, confidencialidade e disponibilidade das informações custodiadas em seus ambientes de atuação, resguardando a conduta de manuseio, controle e proteção das informações contra destruição, modificação, comercialização, divulgação indevida e acessos não autorizados, acidentais ou intencionais, garantindo a continuidade dos serviços a todos os servidores, contribuintes, cidadãos e fornecedores.

2.2. A **IOE**, na busca constante para assegurar a garantia de disponibilidade dos dados e informações, ao

longo dos anos, tem realizado investimentos contínuos em infraestrutura de TI, implementado procedimentos de acordo com os mais elevados padrões tecnológicos e atuado na formação e capacitação de seu corpo técnico. Considerando as informações tratadas no âmbito da autarquia, como ativos valiosos para a eficiente prestação dos serviços públicos; o interesse do cidadão como beneficiário dos serviços prestados pelos órgãos e entidades da administração pública; o dever do estado de proteção das informações pessoais dos cidadãos; a necessidade de incrementar a segurança das redes e bancos de dados governamentais e a necessidade de orientar a condução de políticas de segurança da informação e comunicações já existentes ou a serem implementadas pelos órgãos e entidades da administração pública, cumpre-nos desenvolver ações que viabilizem e assegurem a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações, garantindo a qualidade dos serviços públicos esperados pela população, oferecendo segurança com relação à guarda de "dados sensíveis" pelo governo, através da adoção de medidas rigorosas de segurança para acesso dessas informações.

2.3. A **IOE**, dada sua natureza e responsabilidade como fiel custodiante de sistemas e bases de dados, acessados pelo usuário via internet, precisa assegurar a segurança dos dados e da informação. Partindo-se deste princípio, faz-se mister implantar uma solução de segurança que permita não só controlar os acessos à Internet e acessos externos, mas também que permita o tratamento e remediação de possíveis ataques a rede de dados e serviços da **IOE**.

2.4. A confiabilidade da informação e sua segurança lógica e física são essenciais para os projetos em produção e em andamento na **IOE**. Proteger informações corporativas se tornou um grande desafio devido a constantes e crescentes ameaças. A solução proposta garantirá a privacidade e a disponibilidade dos dados e informações, evitando acessos não autorizados e a parada dos serviços, mitigando o risco de roubo e sequestro de dados e informações sensíveis.

2.5. Baseado neste cenário, a **IOE,** num trabalho conjunto da Presidência com o Núcleo de Tecnologia da Informação - NTI, pesquisou e especificou uma solução de tecnologia da informação de modo a dar continuidade e garantir a qualidade dos serviços prestados e as atividades desta instituição, de forma a abordar um controle de nível de serviço de excelência, garantindo a satisfação dos usuários dos serviços de TI da **IOE**.

2.6. Busca-se, através da presente contratação, atualizar e expandir a atual solução de segurança integrada que tem como objetivo garantir a segurança da informação quanto ao tratamento da segurança dos dados e informações sensíveis, para:

2.6.1. Minimizar os pontos de falha de segurança dos sistemas, informações e dados em custódia, hospedados e processados na **IOE;**

2.6.2. Desenvolver estratégias que possam inibir a tentativa de busca, vazamento e sequestro de informações que possam comprometer a segurança de dados dos órgãos, secretarias, autarquias e funcionários no âmbito da administração pública hospedados na **IOE**;

2.6.3. Permitir o tratamento das informações sensíveis, sujeitas às legislações e normas brasileiras de acordo com os níveis de sigilo, prevenindo ataques ou penalizando repasse ou acesso indevido de informações pela rede de dados da **IOE**;

2.6.4. Reduzir riscos de ataques ao ambiente computacional da **IOE** e buscar estar em conformidade com as normas e padrões de segurança da informação, bem como atendendo aos preceitos legais que regem a responsabilidade sobre os dados gerados, armazenados, tratados e trafegados em ambiente da **IOE**;

2.6.5. Construção de uma base de conhecimento precisa dos acessos realizados aos recursos da rede permitindo detectar, em tempo real, eventuais fraudes ou abusos de utilização;

2.6.6. Maior poder e autonomia da área de segurança no tocante ao gerenciamento dos acessos às áreas, sistemas e aplicações;

2.6.7. Garantir a performance e disponibilidade das aplicações reduzindo a possibilidade de indisponibilidade de acesso aos serviços;

2.6.8. Aumento do sigilo nas informações tratadas em aplicações em rede com a redução de riscos em aplicações;

2.6.9. Aumento da produtividade pelo maior uso de soluções em ambiente tecnológico que facilita e agiliza as ações e a comunicação, devido à confiabilidade no ambiente;

2.6.10. Maior rastreabilidade quanto às tentativas de ataques efetuados dentro do ambiente computacional;

2.6.11. Menores chances de intrusão, vazamento ou sequestro de informações por meio de ataques relacionados a brechas de segurança em aplicações e sistemas operacionais;

2.7. Ainda que a aquisição da Solução se justifique pelo alcance dos propósitos expostos, convém explicitar que sua utilidade vai além destes, podendo ser destacados, ainda:

2.7.1. Controle, auditoria e validação das senhas de alto-privilégio dentro do ambiente da **IOE;**

2.7.2. Monitoração segura e não-intrusiva dos acessos realizados aos recursos na rede;

2.7.3. Minimização dos custos de operação e administração das rotinas de segurança e auditoria;

2.7.4. Maior poder e autonomia da área de segurança no tocante ao gerenciamento dos acessos às área, sistemas e aplicações;

2.7.5. Aumento do sigilo das informações tratadas em aplicações em rede com a redução de riscos de ataques;

2.7.6. Aumento da capacidade de proteção contra ataques á partir de estrutura capaz de escalar de acordo com o crescimento do acesso;

2.7.7. Aumento da produtividade pelo maior uso de soluções em ambiente tecnológico que facilita e agiliza as ações e a comunicação, devido à confiabilidade no ambiente.

2.7.8. Maior rastreabilidade quanto às tentativas de ataques efetuados dentro dos ambientes computacionais;

2.7.9. Menores chances de intrusão, vazamento ou sequestro de informações por meio de ataques relacionados a brechas de segurança em aplicações, sistemas operacionais e senhas de alto-privilégio;

2.7.10. Capacidade de armazenamento centralizado, em cofre digital, das senhas com elevados privilégios de acesso.

3. ESPECIFICAÇÃO DO OBJETO

3.1. Visão Geral

3.1.1. A solução concebida tem por premissa a contratação de um único fornecedor capaz de promover a integração de serviço de plataforma de proteção de perímetro com controle das credenciais de alto-privilégio e a monitoração com possibilidade de contenção, tratamento e mitigação de ataques

avançados ao ambiente, permitindo o gerenciamento da segurança para os dados e informações sensíveis, criando regras aderentes ao negócio, minimizando, assim, os pontos de falha de segurança e garantindo a proteção e disponibilidade dos acessos aos dados e informações sensíveis dos sistemas em custódia, hospedados e processados na **IOE**.

3.1.2. O licenciamento e dimensionamento dos recursos da solução deverão permitir a inclusão ou a descontinuidade de funcionalidades sem perda de performance ou necessidade de troca de hardware.

3.2. Requisitos para dimensionamento

3.2.1. Levando-se em consideração a atual realidade da estrutura física da **IOE**, foram especificadas neste Termo de Referência as prerrogativas de contratação de uma nova solução para proteção dos seus ativos, que deverá contemplar alta disponibilidade, garantindo desempenho e proteção dos acessos aos dados e informações sensíveis dos sistemas e informações em custódia, hospedados e processados no ambiente da **IOE**, permitindo a segregação da rede para aumento da segurança, além de possuir console de gerenciamento para criação e gestão de regras de acesso, visualização de logs e eventos, bem como emissão de relatórios.

3.2.2. A solução será dividida em conjuntos que terão diferentes finalidades, dentre eles:

3.2.2.1. Serviço de proteção de perímetro (WAF – Web Application Firewall);

3.2.2.2. Serviço de plataforma de verificação de ameaças avançadas distribuída em nuvem;

3.2.2.3. Serviço de gestão de senhas de alto privilégio;

3.2.2.4. Fornecimento, instalação e configuração de appliances em cluster com 02 dispositivos UTM, com suporte a conexões de 2 Gbps e controle de aplicação habilitado para todas as assinaturas, conforme necessidades do ambiente computacional;

3.2.2.5. Migração das regras de firewall atualmente implementadas para os novos equipamentos;

3.2.2.6. Serviço de instalação e configuração de softwares;

3.2.2.7. Avaliação e Suporte Técnico para operação do sistema com repasse tecnológico;

3.2.2.8. Serviços de Monitoração 24 x 7 x 365 de toda a solução contratada;

3.3. Escopo da Solução

3.3.1. Caso ocorram ataques avançados e outros malwares sofisticados, todos os segmentos de rede da **IOE** ficarão vulneráveis. Com a atualização da solução de firewall e acréscimo da proteção do perímetro na nuvem, estaremos aumentando o nível de segurança dos serviços ofertados na rede da **IOE**, através de tecnologia atualizada e robusta.

3.4. Solução de Serviços Integrados

3.4.1. A solução contém serviços integrados baseado em appliances locais e em nuvem conforme abaixo:

ITEM	DESCRIÇÃO	MÉTRICA	Qtd.	VALOR UNITÁRIO ESTIMADO	VALOR TOTAL ESTIMADO
1	Fornecimento de Firewall UTM composto por 01 Cluster com 02 (dois) appliances para ambiente de internet, com licenças de Antivirus, AntiSPAM, VPN, Web Filtering, IPS, Integração com o serviço de diretórios e LOG's.	Hardware	1	R$165.300,00	R$ 165.300,00
2	Licenciamento de serviço de plataforma de proteção de perímetro (WAF – Web Application Firewall)	Software	1	R$ 119.000,00	R$ 119.000,00
3	Licenciamento de solução integrada anti-ransomware, tratando a segurança de rede e e-mail	Software	1	R$ 402.000,00	R$ 402.000,00
4	Licenciamento de software de gestão de Senhas de Alto Privilégio	Software	1	R$ 447.900,00	R$ 447.900,00

5	Prestação de serviços de avaliação técnica, implantação, configuração, migração e treinamento	Serviço	1	R$ 347.400,00	R$ 347.400,00
6	Prestação de serviços de monitoramento contínuo em regime 24x7x365, atualizações, suporte técnico e garantia	Serviço	12	R$ 63.200,00	R$ 758.400,00
VALOR TOTAL ESTIMADO				R$ 2.240.000,00	

4. ESPECIFICAÇÃO TÉCNICA DA SOLUÇÃO

4.1. Características Gerais da Solução Integrada de Segurança

4.1.1. As especificações técnicas apresentadas nos subitens a seguir, contemplam as necessidades exigidas para o funcionamento do ambiente operacional desta entidade na atualidade, através do atributo de solução, visa manter a compatibilidade e a evolução tecnológica do fabricante.

4.1.2. O serviço a ser prestado consiste essencialmente da disponibilização e ativação de uma plataforma de proteção de perímetro, proteção de aplicativos Web, proteção contra ameaças avançadas através da rede e e-mails, em conjunto com proteção e controle de senhas de alto privilégio;

4.1.3. Os equipamentos propostos devem ser novos, ou seja, de primeiro uso; e estar na linha de produção do fabricante (não podem estar em end-of-life ou end-of-support);

4.1.4. A CONTRATADA deverá garantir a atualização do software embarcado e sistema operacional de todos os componentes previstos na proposta durante o período de 12 meses;

4.1.5. No preço deverá estar incluído todo o software e hardware necessário para atender as características exigidas, bem como as atualizações para todas as versões do produto que forem lançadas durante o período do contrato;

4.1.6. Características gerais da plataforma de proteção de perímetro de aplicativos Web;

4.1.7. Deverá prover segurança "*As a Service* " para Aplicações Web;

4.1.8. Deverá possuir nuvem de segurança como uma camada de infraestrutura de alta performance e abrangência mundial posicionada entre os servidores da **IOE** e os usuários que acessam o site ou portal;

4.1.9. Deverá prover proteção contra ataques em nível de Rede (camadas 3 e 4): ICMP, TCP e UDP floods;

4.1.10. Deverá prover proteção contra ataques em nível de aplicação (camada 7): HTTP flood, Bruteforce;

4.1.11. Deverá possuir infraestrutura global de mitigação;

4.1.12. Deve estar em conformidade com PCI-DSS (6.6);

4.1.13. Deverá prover proteção contras as ameaças OWASP TOP 10;

4.1.14. Deverá prover disponibilidade mínima de 99.999%;

4.1.15. Deverá suportar regras Customizadas;

4.1.16. Deverá prover gestão de acesso às áreas restritas do site;

4.1.17. Deverá prover proteção sem intervenção no código da aplicação;

4.1.18. Deverá ser capaz de funcionar via SMS, Google Authenticator ou E-mail;

4.1.19. Deverá Impedir a instalação de Backdoors;

4.1.20. Deverá detectar e bloquear Backdoors previamente instalados;

4.1.21. Deverá buscar por incidências nas principais Blacklists;

4.1.22. Ser capaz de detectar e gerenciar acesso de Bots;

4.1.23. Permitir o acesso somente de Bots legítimos (Google, Facebook, Pingdom);

4.1.24.Deverá prover *Caching* de conteúdo estático e dinâmico;

4.1.25. Deverá prover compressão de imagens e arquivos de textos (js, html, css);

4.1.26. Deverá prover renderização progressiva de imagens;

4.1.27. Deverá prover operação assistida de forma remota de toda solução;

4.1.28. Deverá prover o monitoramento e suporte 24x7x365;

4.1.29. Deverá prover resposta a incidentes;

4.1.30. Deverá prover geração de alertas;

4.1.31. Acompanhamento de realização de deploys para correção ou novas versões;

4.1.32. Apoiar a equipe de desenvolvimento em testes e outras atividades que envolvem a infraestrutura das aplicações Web;

4.1.33. Monitorar o correto funcionamento e performance das aplicações Web no tocante aos serviços contratados;

4.1.34. Sugerir e alertar sobre ações ou atividades que possam impactar positivamente ou negativamente no funcionamento das aplicações Web;

4.1.35. Realizar monitoramento de disponibilidade, funcionamento e performance do serviço WAF em regime 24x7x365, incluindo fins de semana e feriados;

4.1.36. O monitoramento deverá captar dados em tempo real para que a contratada possa atuar de forma proativa no sentido de prever e minimizar possíveis falhas;

4.1.37. O serviço deverá atuar de forma preventiva e proativa no sentido minimizar possíveis falhas das aplicações, mantendo sempre comunicação assertiva e transparente com a contratada;

4.1.38. Os serviços serão prestados remotamente, porém a equipe da contratada deverá estar à disposição para eventuais compromissos como reuniões ou serviços de implantação e manutenção.

4.2. Características gerais do cluster com 02 (dois) appliances de firewall UTM e licenciamento

4.2.1. O equipamento deve se instalar em rack com largura padrão 19 polegadas, padrão EIA-310, ocupando no máximo 1U (44mm) do referido rack;

4.2.2. Deverão ser fornecidos todos os cabos, suportes (se necessários, "gavetas", "braços" e "trilhos") para a instalação do equipamento no rack;

4.2.3. Possuir painel frontal do tipo LCD com capacidade de apresentar informações a respeito da utilização de CPU, memória e tráfego de rede do equipamento;

4.2.4. Dispor de fonte de alimentação com tensão de entrada de 110V a 220V AC automática e frequência de 60Hz;

4.2.5. As interfaces de rede deverão estar localizadas, na frente do equipamento;

4.2.6. Possuir pelo menos 8 (oito) interfaces de rede Gigabit Ethernet 10/100/1000 com leds indicativos de link e atividade;

4.2.7. Possuir painel/led indicativo de on/off do uso de disco e interfaces de rede;

4.2.8. Possuir um Throughput mínimo de 2000 (Dois mil) Mbps para tráfego comum;

4.2.9. Possuir um Throughput mínimo de 1800 (Um Mil e Oitocentos) Mbps para tráfego criptografado (AES-128);

4.2.10. Possuir um Throughput mínimo de 1000 (um Mil) Mbps para tráfego de IPS/IDS;

4.2.11. Possuir no mínimo 4 (quatro) GB de memória RAM, e permitir expansão para até 8 (oito) GB;

4.2.12. Capacidade de estabelecer no mínimo 3000 (três mil) túneis VPN simultaneamente;

4.2.13. Deverá fornecer no mínimo 50 (cinquenta) licenças para conexões simultâneas de clientes VPNs (client-to-server);

4.2.14. A base de assinaturas do módulo de IPS deverá possuir no mínimo 3.500 (três mil e quinhentos) ataques conhecidos;

4.2.15. A base de assinaturas do módulo de Antivírus deverá possuir no mínimo 3.000.000 (três milhões) malwares conhecidos;

4.2.16. Suportar 1.500.000 (um milhão e quinhentos mil) conexões simultâneas;

4.2.17. Possuir dispositivo de armazenamento interno do tipo SSD (Solid-State Drive) de no mínimo 240 (duzentos e quarenta) GB;

4.2.18. Possuir uma interface para configuração e gerenciamento através de interface de linha de comando CLI (Command Line Interface);

4.2.19. O console do equipamento deverá ser acessado utilizando interface física específica para esta finalidade, do tipo serial DB-9, com conector RS-232 ou RJ-45;

4.2.20. O dispositivo deverá trabalhar com o conceito de refrigeração túnel de vento, possibilitando assim melhor refrigeração do dispositivo, desta forma prolongando sua vida útil;

4.2.21. O fluxo de ar deverá obrigatoriamente ser: entrada de ar frio pela frente, saída de ar quente por trás do dispositivo;

4.2.22. O sistema de coolers deverá ser do tipo gaveta removível, permitindo sua retirada ou inserção sem o uso de ferramentas;

4.2.23. Possuir pelo menos 2 (duas) portas USB para inserção de dispositivos externos;

4.2.24. No caso da porta(s) USB o equipamento deverá registrar as atividades de uso desta(s) porta(s), registrando informações, tais como: usuário que ativou ou desativou a porta, data e hora de ativação, etc.

4.2.25. Atualização do sistema operacional embarcado durante o período de 12 meses;

4.2.26. No preço deverá estar incluído todo o software necessário para atender as características exigidas, bem como as atualizações para todas as versões do produto que forem lançadas durante o período do contrato;

4.2.27. Atualização do software embarcado durante o período de 12 meses;

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

Linux ou FreeBSD;

4.2.29. Efetuar controle de tráfego por estado no mínimo para os protocolos TCP, UDP e ICMP baseados nos endereços de origem, destino e porta;

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

4.2.31. Suportar o Internet Protocol Versões 6 (IPv6), deverão estar em conformidade com as RFCs listadas abaixo:

4.2.31.1. RFC2460 - Internet Protocol, Version 6 (IPv6) Specification;

4.2.31.2. RFC4291 - IP Version 6 Addressing Architecture;

4.2.31.3. RFC3484 - Default Address Selection for Internet Protocol version 6 (IPv6);

4.2.31.4. RFC4443 - Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification;

4.2.31.5. RFC4862 - IPv6 Stateless Address Autoconfiguration;

4.2.31.6. RFC1981 - Path MTU Discovery for IP version 6;

4.2.31.7. RFC4861 - Neighbor Discovery for IP version 6 (IPv6);

4.2.31.8. RFC4213 - Basic Transition Mechanisms for IPv6 Hosts and Routers.

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

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

4.2.34. Dispõe de servidor DHCP interno e permite DHCP relay;

4.2.35. Suportar PIM (Protocol Independent Multicast);

4.2.36. Suportar o protocolo Distance-Vector Multicast Routing Protocol (DVMRP);

4.2.37. Pode ser integrado com servidores de Network Time Protocol (NTP);

4.2.38. Suporta funcionar em modo BRIDGE (transparente mode) esta funcionalidade permite que o Firewall funcione em modo transparente/oculto na rede, impossibilitando sua identificação, otimizando o tempo de configuração e diminuindo a intervenção humana neste processo;

4.2.39. Capacidade para trabalhar com conversão de endereços e portas (NAT/NAPT) conforme RFC 3022;

4.2.40. Suportar no mínimo os seguintes protocolos de roteamento dinâmico IPv4: RIP1, RIP2, OSPF e BGP;

4.2.41. O equipamento deverá suportar o registro do dispositivo dinamicamente, pelo seu endereço IP de WAN, em pelo menos 5 (cinco) provedores de serviços de DDNS;

4.2.42. Possuir e fornecer manual escrito em português do Brasil e em mídia eletrônica para todos os equipamentos e softwares componentes da solução;

4.2.43. Possuir mecanismo de forma a possibilitar o funcionamento transparente dos protocolos FTP, Real Áudio, Real Vídeo, RTSP, H.323 e PPTP mesmo quando acessados por máquinas através de conversão de endereços. Este suporte deve funcionar tanto para acessos de dentro para fora quanto de fora para dentro;

4.2.44. Possuir interface em português do Brasil;

4.2.45. Prover autenticação de usuários para os serviços Telnet, FTP, HTTP, HTTPS e Gopher, utilizando as bases de dados de usuários e grupos de servidores Windows e Unix, de forma simultânea;

4.2.46. Permitir a utilização de LDAP, LDAP/SSL, LDAP/TLS, RADIUS, hardware tokens (SecureID ou equivalente), certificados X.509 (gravados em disco e/ou em tokens criptográficos/smartcards) e sistema S/KEY para a autenticação de usuários;

4.2.47. Permitir o cadastro dos usuários e grupos em base de dados própria por meio da interface de gerencia remota do dispositivo;

4.2.48. Permitir a integração com qualquer autoridade certificadora emissora de certificados X509 que seguir o padrão de PKI descrito na RFC 2459, inclusive verificando as CRLs (Certificates Revogation Lists) emitidas periodicamente pelas autoridades, que devem ser obtidas automaticamente pelo

dispositivo via protocolos HTTP e LDAP;

4.2.49. Permitir o controle de acesso por usuário, para plataformas Windows NT, 2000, 2003, 2008, XP, Vista, Windows 7 e Windows 8 de forma transparente (sem a necessidade de o usuário digitar novamente a senha), para todos os serviços suportados, de forma que ao efetuar o logon na rede, um determinado usuário tenha seu perfil de acesso automaticamente configurado e sem a necessidade de qualquer agente instalado no desktop do usuário;

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

4.2.51. Possuir perfis de acesso hierárquicos;

4.2.52. Permitir a atribuição de perfil de acesso à usuário ou grupo de usuários de acordo com o endereço ou range IP do equipamento que o usuário esteja utilizando;

4.2.53. Deverá possuir suporte para autenticação em ambientes Citrix e Terminal Service, permitindo diferenciar 2 (dois) ou mais usuários autenticados no mesmo servidor/máquina, por meio da conexão protocolo por usuário;

4.2.54. A funcionalidade de Captive Portal deverá suportar a instalação em um servidor externo a solução de Firewall;

4.2.55. Deverá oferecer recurso de Captive Portal compatível com autenticação em AD, LDAP e RADIUS e em base de dados de usuários interna para autenticação de usuários visitantes/temporários (acesso guest);

4.2.56. A solução deverá possuir gerenciamento Web com possibilidade de criar usuários locais ou integração com uma base externa LDAP;

4.2.57. Deverá possuir suporte ao protocolo NTP e poderá permitir cadastrar até 4 servidores distintos;

4.2.58. A solução deverá permitir o backup de suas configurações e posterior restore;

4.2.59. A solução deverá permitir em seu portal de autenticação, cadastro de novos usuários e integração com bases externas de usuários Facebook, Google, Twitter, Linkedin;

4.2.60. Deverá suportar no mínimo os seguintes métodos de autenticação:

4.2.60.1. Active Directory

4.2.60.2. Apache htpasswd file

4.2.60.3. Email

4.2.60.4. Facebook (OAuth 2)

4.2.60.5. Github (OAuth 2)

4.2.60.6. Google (OAuth 2)

4.2.60.7. Kerberos

4.2.60.8. LDAP

4.2.60.9. LinkedIn (OAuth 2)

4.2.60.10. RADIUS

4.2.60.11. SMS

4.2.60.12. Sponsored Email

4.2.60.13. Windows Live (OAuth 2)

4.2.61. Se for um usuário visitante e não for possível consultar uma base de autenticação o Captive Portal deverá solicitar informações para cadastro e o sistema irá enquadrar o usuário em um perfil de acesso;

4.2.62. Deverá permitir selecionar qual segmento de rede irá utilizar a funcionalidade de Captive Portal;

4.2.63. O sistema deverá criar uma regra de filtragem que libere o acesso dos usuários visitantes para a internet por até 10 minutos para os serviços HTTP, HTTPS, POP3, POP3S, IMAP, IMAPS;

4.2.64. A solução de Captive Portal poderá ser instalada em uma máquina/appliance virtual, compatível com VMware ou Hyper.

4.2.65. Permitir o agrupamento das regras de filtragem por política;

4.2.66. Prover mecanismo que permita a especificação de datas de validade inicial e final, para regras de filtragem, individualmente (por regra);

4.2.67. Prover mecanismo que permita a especificação da validade para regras de filtragem, individualmente (por regra), por dia da semana e horário;

4.2.68. Permitir a visualização pela interface gráfica, em tempo real, de todas as conexões TCP e sessões UDP ativas através do dispositivo e a finalização de qualquer uma destas sessões ou conexões;

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

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

4.2.71. Possuir mecanismo que permita capturar o tráfego de rede em tempo real (sniffer) via interface gráfica, com visualização em tempo real pela interface gráfica e com capacidade para exportação dos dados capturados para arquivo no mínimo em formato PCAP;

4.2.72. Deverá permitir configurar por serviço (TCP ou UDP), o tempo limite (timeout) diferente para o descarte de conexões ociosas;

4.2.73. Deverá possuir a capacidade de habilitar ou desabilitar regras de filtragem baseado na disponibilidade do link de dados;

4.2.74. A utilização da funcionalidade de captura de pacotes (sniffer) não deverá causar nenhuma queda de desempenho (throughput) do equipamento;

4.2.75. Permitir configuração de filtros para a captura do tráfego em tempo real, no mínimo por protocolo, endereço IP de origem e/ou destino e porta de origem e/ou destino, utilizando para tanto linguagem textual;

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

4.2.77. Permitir a execução de até oito capturas de tráfego em tempo real simultaneamente, inclusive em pontos diferentes ou com filtros diferentes;

4.2.78. Prover mecanismo contra ataques de falsificação de endereços (IP Spoofing) através da especificação da interface de rede pela qual uma comunicação deve se originar;

4.2.79. Prover proteção contra os ataques de negação de serviço SYN Flood, Land, Tear Drop e Ping O'Death;

4.2.80. Possuir mecanismo que limite o número máximo de conexões simultâneas de um mesmo cliente para um determinado serviço e/ou servidor;

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

4.2.82. Permitir integração com sistema detecção de intrusão (IDS) externo, permitindo que esses agentes insiram regras temporárias no dispositivo em caso de detecção de algum ataque, com duração pré-determinada, de forma automática;

4.2.83. Possuir sistema de prevenção de intrusão (IPS) nativo, permitindo o bloqueio do ataque em caso de detecção do mesmo;

4.2.84. Possuir filtro de aplicações de modo a permitir a identificação de padrões de dados dentro das conexões, possibilitando o tratamento automático (bloqueio, liberação ou redução/aumento de banda) de aplicações do tipo peer-to-peer, de download de arquivos, entre outros;

4.2.85. Possuir Proxy nativo para tráfego HTTP, HTTPS, SIP, H323, FTP, SMTP, POP3, IMAP, RTSP, Real Áudio, DCE-RPC, PPTP e TELNET;

4.2.86. Possuir proxy SOCKS, permitindo que clientes da versão 4 e 5 deste protocolo acessem a Internet através do dispositivo;

4.2.87. Possuir mecanismo de filtragem de serviços RPC pelo nome do serviço ou, no caso de serviço sem nome pré-definido, pelo seu número;

4.2.88. O Proxy IMAP deverá permitir criar regras de filtro por tipo MIME e pelo nome do arquivo

anexado da mensagem de e-mail;

4.2.89. Deverá fazer a verificação do modulo de antivírus no protocolo IMAP mesmo em conexão SSL;

4.2.90. O Proxy IMAP deve permitir remover o anexo infectado da mensagem de e-mail;

4.2.91. Permitir que anexos malformados sejam removidos pelo Proxy IMAP;

4.2.92. O Proxy IMAP deverá permitir que o administrador do Firewall possa habilitar as seguintes opções:

4.2.92.1. Permitir ou não anexos malformados;

4.2.92.2. Ignorar erros do antivírus;

4.2.92.3. Remover arquivos cifrados;

4.2.92.4. Remover arquivos corrompidos;

4.2.93. Possibilitar o gerenciamento completo e a implantação de quotas para navegação web a um determinado usuário ou a um grupo de usuários, de acordo com o perfil de acesso, sendo baseada em volume de dados ou em tempo de utilização do serviço;

4.2.94. O Proxy HTTP deverá possuir mecanismo que bloqueie Banners, ActiveX, Java, Javascript, e ainda tentativas de navegação informando na URL apenas o número IP;

4.2.95. Permitir visualização dos sites acessados em tempo real;

4.2.96. Permitir a inclusão de macros enviada para a página de redirecionamento (no caso de bloqueio de categorias) com a categoria na qual o site bloqueado se encontrava;

4.2.97. Permitir a inserção de uma URL de redirecionamento para bloqueio por palavras-chave nas regras de perfil para HTTP, FTP, Gopher e tipos de arquivos bloqueados;

4.2.98. Permitir a filtragem de URLs, para os protocolos HTTP, HTTPS, FTP e Gopher, por usuário, permitindo a definição de perfis de acesso diferenciados para cada usuário ou grupo;

4.2.99. Capaz de operar em modo man-in-the-middle para conexões do tipo HTTPS para controle de

acesso e bloqueio a categorias;

4.2.100. Suportar a filtragem do protocolo HTTPS pelo campo “CommonName” e do “Server Name Indication Extension” do certificado digital;

4.2.101. Permitir a remoção de anúncios em páginas HTML, sem que as mesmas percam formatação ou apresentem mensagens de erro;

4.2.102. Implementar Proxy transparente para o protocolo HTTP e HTTPS, de forma a dispensar a configuração dos browsers das máquinas clientes para a utilização das características dos dois itens acima;

4.2.103. Possuir funcionalidade de bloquear ou liberar a navegação web dependendo do navegador (browser) que o usuário estiver utilizado;

4.2.104. Implementar sistema que possibilite a reescrita de URLs;

4.2.105. Implementar sistema que possibilite a concatenação (Stripping) de cabeçalho HTTP;

4.2.106. Implementar sistema que possibilite a adição de cabeçalho HTTP;

4.2.107. Possuir mecanismo de proxy SSL reverso, permitindo que VPNs cliente-servidor sejam estabelecidas com o dispositivo, de forma transparente, e então redirecionadas para qualquer servidor interno da rede, sem o uso de cliente de criptografia específico e com autenticação opcional de usuários via certificados digitais padrão X.509;

4.2.108. Permitir o uso certificados digitais com chaves de tamanho até 4096 bits no proxy SSL reverso;

4.2.109. Possuir mecanismo que limite opcionalmente o uso do proxy SSL reverso para serviços e servidores específicos de acordo com perfis de acesso atribuídos a usuários e grupos de usuários;

4.2.110. Permitir o controle de acesso por usuário e grupos para controle de IMs como Skype, Google Talk, Yahoo Messenger e Facebook Messenger.

4.2.111. Possui a capacidade de identificar o tráfego Web e classifica-lo de acordo com as aplicações e sub aplicações trafegando na rede, tais como redes sociais: Facebook, Google+, Twitter, etc; de comunicação: Skype, Gmail, GTalk, etc;

4.2.112. Permite 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 Ultrasurf, Skype e ataques mediante a porta 443;

4.2.113. Suporta a detecção de aplicações dinâmicas dentro de sessões de proxy HTTP;

4.2.114. Deve permitir o armazenamento em Cache de conteúdo trafegados pelo protocolo HTTP e HTTPS;

4.2.115. Possuir sistema de cache interno, armazenando requisições WEB em disco local;

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

4.2.117. Possibilitar a integração com cache WEB externos hierárquicos utilizando ICP (Internet Cache Protocol);

4.2.118. Possuir a funcionalidade de eliminar o conteúdo do Cache (limpar o Cache);

4.2.119. Prover serviço VPN (Virtual Private Network) para pacotes IP e VPN SSL, com chaves de criptografia com tamanho igual ou superior a 128 bits, de forma a possibilitar a criação de canais seguros ou VPNs através da Internet;

4.2.120. Suportar padrão IPSEC, de acordo com as RFCs 2401 a 2412, de modo a estabelecer canais de criptografia com outros produtos que também suportem tal padrão;

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

4.2.122. Mostrar, em tempo real, um gráfico de uso das VPNs IPSEC estabelecidas, permitindo auferir o tráfego em cada uma delas e as SPIs negociadas e ativas;

4.2.123. Possibilitar mecanismo de criação de VPNs entre máquinas Windows NT, 2000, 2003, XP, Vista, Windows 7, Windows 8, Linux e Mac OS e o dispositivo, com chaves de criptografia simétricas com tamanho igual ou superior a 128 bits;

4.2.124. Funcionar como um provedor de VPN para clientes, de modo a atribuir aos clientes endereços IPs das redes internas, colocando-os, virtualmente, dentro das mesmas (0 hops);

4.2.125. Prover cliente VPN para as plataformas Windows 2000, 2003, XP, Vista, Windows 7, Windows 8 e Linux, que permita uso de chaves criptográficas simétricas com 128 ou mais bits;

4.2.126. O cliente de tunelamento de rede IP deverá ser, para clientes Windows e Linux, executar com privilégios básicos de usuário comum. Esta funcionalidade não é exigida apenas durante a primeira instalação do cliente;

4.2.127. Deverá ser possível configurar o endereço/range IP a ser atribuído a placa de rede virtual do cliente de VPN, bem como sua máscara de rede, endereços dos servidores DNS, endereço dos servidores WINS, rota default e rotas para sub-redes;

4.2.128. No VPN cliente/firewall deverá ser possível a configuração do envio ou não de pacotes broadcast da rede onde o servidor se encontra para o cliente;

4.2.129. O cliente de VPN deverá possibilitar que seu funcionamento seja sincronizado ou não com o dial-up do Windows, possibilitando que ele estabeleça a VPN automática e imediatamente depois de se ter estabelecido uma conexão discada;

4.2.130. Na VPN cliente/firewall deve ser possível especificar e fixar quais são as portas usadas na comunicação entre o cliente e o servidor;

4.2.131. Suportar VPN Failover (re-estabelecimento da VPN sobre um segundo enlace caso haja falha no enlace principal);

4.2.132. A solução de VPN deverá trabalhar no mínimo com os seguintes protocolos: IPSEC, OpenVPN, PPTP, L2TP, SSL;

4.2.133. Possuir funcionalidade Dead Peer Detection (DPD), ou similar;

4.2.134. Prover funcionalidade de VPN SSL, com o estabelecimento do túnel VPN e autenticação via browser;

4.2.135. A conexão VPN SSL deverá ser totalmente transparente para o usuário final, de forma que seja realizado o download e instalação do Applets, assim que necessários;

4.2.136. Deve ter a capacidade para fazer o download do Software Client da VPN SSL direto do dispositivo;

4.2.137. Disponibilidade de Software SSL-Client para no mínimo: Windows XP, Windows Vista, Windows 7, Windows 8, Linux e Mac OS;

4.2.138. Deverá permitir a integração de algoritmos de terceiros em seus sistemas criptográficos sem intervenção de terceiros, Hardware ou Software, sujeito exclusivamente as normas Brasileiras.

4.2.139. Possuir capacidade de integração de algoritmos de estado, em hardware, em seu sistema criptográfico, sujeito exclusivamente as normas Brasileiras.

4.2.140. Possuir suporte ao protocolo SNMP (v1, 2 e 3), através de MIB2;

4.2.141. Permitir em tempo real a visualização de estatísticas do uso de CPU, memória do dispositivo, bem como o tráfego de rede em todas as interfaces do dispositivo através da interface gráfica remota, de forma gráfica ou em tabelas;

4.2.142. Caso o dispositivo utilize agentes externos para divisão de processamento (antivírus, filtro de conteúdo, IDS ou AntiSpam) o dispositivo deverá permitir a verificação em tempo real da comunicação com estes agentes;

4.2.143. Possuir sistema de alerta que informe o administrador através de e-mails, janelas de alerta na interface gráfica, execução de programas e envio de traps SNMP;

4.2.144. Deverá permitir que os e-mails de alerta sejam encaminhados com autenticação (com suporte a conexões seguras TLS pelo Cliente SMTP “MSMTP”) ou sem autenticação (usando a porta 25, padrão para o protocolo SMTP);

4.2.145. Permitir a criação de perfis de administração baseado em papéis (role-based), de forma a possibilitar a definição de diversos administradores para o dispositivo, cada um responsável por determinada tarefa da administração;

4.2.146. Permitir a conexão simultânea de vários administradores, sendo apenas um deles com poderes de alteração de configurações e os demais apenas de visualização das mesmas;

4.2.147. Permitir que o segundo administrador ao se conectar possa enviar uma mensagem ao primeiro através da interface de administração;

4.2.148. Fornecer gerência remota, com interface gráfica nativa, através de canal criptografado com chave

de criptografia igual ou superior a 128 bits, para plataformas Windows Me, Windows NT/2000/XP/2003/2008/Vista/Windows 7/Windows 8 e Linux;

4.2.149. Capacidade para criação de entidades/objetos, que podem ser um IP, um range IP ou um dispositivo, etc. para facilitar a administração;

4.2.150. Possibilitar drag-and-drop (arrastar e soltar) para criação e alteração de regras, por meio da interface gráfica;

4.2.151. A interface gráfica deverá possuir mecanismo que permita a gerência remota de múltiplos dispositivos sem a necessidade de se executar várias interfaces;

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

4.2.153. Possuir mecanismo que permita a realização de cópias de segurança (backups) e restauração remota, através da interface gráfica, sem necessidade do reinício do sistema;

4.2.154. Deverá ser capaz de executar um backup por linha de comando e oferecer a opção de salvar o arquivo de backup localmente ou exportar usando o protocolo FTP;

4.2.155. Possuir mecanismo que possibilite a aplicação de correções e atualizações para o dispositivo de forma remota por meio da interface gráfica;

4.2.156. Possuir mecanismo anti-suicídio para a administração remota, evitando que o administrador perca o acesso ao dispositivo por uma configuração incorreta;

4.2.157. Permitir integração com produto de gerenciamento centralizado de múltiplos dispositivos;

4.2.158. Possuir interface orientada a linha de comando (Command Line Interface) para a administração do dispositivo a partir do console;

4.2.159. Suportar o rollback (voltar para a versão anterior) de patches aplicados;

4.2.160. Prover mecanismo de consulta às informações registradas (logs) por meio da interface gráfica de administração;

4.2.161. Possibilitar o armazenamento de seus registros (log e/ou eventos) em máquina remota em plataformas Windows Server (NT/2000/2003/2008) ou Unix, através de protocolo criptografado ou SYSLOG;

4.2.162. Possibilitar a geração de pelo menos os seguintes tipos de relatório, publicados em formato HTML, TXT e PDF:

4.2.162.1. Máquinas mais acessadas;

4.2.162.2. Serviços mais utilizados;

4.2.162.3. Usuários que mais utilizaram serviços;

4.2.162.4. URLs mais visualizadas;

4.2.162.5. Categorias Web mais acessadas (em caso de existência de um filtro de conteúdo Web);

4.2.162.6. Categoria do site bloqueado (em caso de existência de um filtro de conteúdo Web);

4.2.162.7. Downloads realizados;

4.2.162.8. Downloads bloqueados;

4.2.162.9. Endereço IP acessado pelo proxy Web;

4.2.162.10. Endereço IP bloqueado pelo proxy Web;

4.2.162.11. Quota – bytes consumidos;

4.2.162.12. Quota – tempo consumidos;

4.2.162.13. Sites acessados;

4.2.162.14. Sites Bloqueados;

4.2.162.15. Maiores emissores/receptores de e-mail;

4.2.162.16. Possibilitar a geração de pelo menos os seguintes tipos de relatório com cruzamento de

informações, mostrados em formato HTML, TXT e PDF:

4.2.162.17. Máquinas acessadas X serviços bloqueados;

4.2.162.18. Usuários X URLs acessadas;

4.2.162.19. Usuários X categorias Web bloqueadas (quando utilizado com filtragem de conteúdo Web);

4.2.163. Possibilitar a geração dos relatórios dos itens acima sob demanda e através de agendamento diário, semanal, mensal, período específico ou por demanda pelo menos nos formatos HTML, TXT e PDF;

4.2.164. Permitir publicação automatizada dos relatórios utilizando FTP em pelo menos três equipamentos distintos;

4.2.165. Permitir exportação dos registros (logs) no mínimo em formato TXT e CSV;

4.2.166. Implementar mecanismo de divisão justa de largura de banda (QoS), permitindo a priorização de tráfego por regra de filtragem, por usuário ou ainda priorizando acesso a sites por categoria ou palavra-chave;

4.2.167. Implementar mecanismo de limitação de banda através da criação de canais virtuais, permitindo que os mesmos serem alocados por regra de filtragem e por usuário;

4.2.168. Permitir modificação (remarcação) de valores DSCP para o DiffServ;

4.2.169. Implementar no mínimo 07 classes de serviço distintas, com configuração do mapeamento e marcação para códigos DSCP através da interface gráfica;

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

4.2.171. Suportar o uso simultâneo de múltiplos links em um mesmo firewall, de provedores distintos ou não, sendo o firewall o responsável por dividir o tráfego entre os distintos links;

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

4.2.173. Implementar mecanismo de balanceamento de carga, permitindo com que vários servidores internos, sejam acessados externamente pelo mesmo endereço IP. O balanceamento de canal deverá monitorar os servidores internos e, em caso de queda de um destes, dividir o tráfego entre os demais, automaticamente;

4.2.174. Implementar mecanismo de persistência de sessão para o balanceamento de carga, através de diversas conexões, para quaisquer protocolos suportados pelos servidores sendo balanceados;

4.2.175. O balanceamento de carga deverá ainda possibilitar que os servidores sejam monitorados através do protocolo ICMP ou conexão TCP em porta configurável;

4.2.176. Quando o monitoramento ocorrer no protocolo ICMP deverá permitir inserir até 3 (três) verificadores e somente o link será marcado como inativo se o 3 (três) pararem de responder;

4.2.177. Deverá possuir no mínimo as seguintes políticas de balanceamento de tráfego entre os links:

4.2.178. Permitir dividir o tráfego entre os links por porcentagem de utilização dos mesmos;

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

4.2.180. Deverá permitir direcionar um tráfego para o link que tiver mais conexões ativas;

4.2.181. Permitir direcionar o tráfego para o link com a menor latência, baseado no tempo de resposta de um domínio inserido pelo administrador do firewall;

4.2.182. Deverá possuir as seguintes opções de configurações para o monitoramento do link que fazem parte do balanceamento de link:

4.2.182.1. Intervalo de monitoramento;

4.2.182.2. Quantidade de falhas necessárias antes de marcar o link como inativo;

4.2.182.3. Quantidade de sucesso necessário antes de marcar o link como ativo;

4.2.182.4. Intervalo de tempo necessário antes de calcular o balanceamento do tráfego entre os links.

4.2.183. A solução deve suportar funcionamento com 2 (dois) ou mais equipamentos idênticos, de forma que funcione com tolerância a falhas (ativo/passivo) ou alta performance (ativos/ativos), onde poderá trabalhar no mínimo de duas formas, de acordo com a necessidade da instalação. Sendo elas:

4.2.184. Os dois dispositivos são ligados em paralelo, com réplicas do estado de conexões entre eles. O dispositivo secundário não estará tratando o tráfego, ele entrará em funcionamento para tratamento de tráfego somente quando o dispositivo principal cair, sem que se tenha perda de conexão, de canal VPN, usuários autenticados e IPs bloqueados pelo IPS/IDS;

4.2.185. Dois ou mais dispositivos devem estar em funcionamento simultaneamente, balanceando o tráfego de rede entre eles de forma automática e replicando configuração, estado das conexões entre eles e também de forma automática, sem que se tenha perda de conexão, de canal VPN, usuários autenticados e IPs bloqueados pelo IPS/IDS em caso de falha de algum equipamento. Nesta modalidade, podem ser colocados até 64 firewalls em paralelo;

4.2.186. Deverá ser capaz de manter o sincronismo entre as seguintes configurações como Regras de Firewall, Regras de NAT, Entidades, Contas administrativas, Configuração de VPN, Configurações de rede, Roteamento estático, Roteamento dinâmicas, Perfis e bases de antivírus, filtros web, AntiSpam e IDS/IPS;

4.2.187. Possuir sistema de prevenção de intrusão (IPS) nativo, permitindo sejam inseridas regras temporárias no firewall em caso de detecção de algum ataque, com duração pré-determinada, de forma automática;

4.2.188. A base de assinaturas do sistema de IPS nativo deverá ser fornecida pelo período do contrato;

4.2.189. Possuir filtro de aplicações de modo a permitir a identificação de padrões de dados dentro das conexões, possibilitando o tratamento automático (bloqueio, liberação ou redução/aumento de banda) de aplicações do tipo peer-to-peer, de download de arquivos, entre outros;

4.2.190. Deverá suportar fragmentação e desfragmentação IP;

4.2.191. Deverá implementar detecção de protocolos independentemente da porta utilizada;

4.2.192. Deverá possibilitar a resposta há eventos com TCP Reset ou descarte de pacotes;

4.2.193. Possuir modo de Inspeção baseados em regras e assinaturas;

4.2.194. Metodologias de detecção Multidimensional:

4.2.195. Assinaturas (Impressões Digitais) do Ataque.

4.2.196. Anomalias no Protocolo.

4.2.197. Anomalias no Comportamento.

4.2.198. Sistema de prevenção de intrusão (IPS) nativo, permitindo sejam inseridas regras temporárias no firewall UTM em caso de detecção de algum ataque, com duração pré-determinada, de forma automática;

4.2.199. A base de assinaturas do sistema de IPS e DPI nativo deverá ser fornecida pelo período do contrato;

4.2.200. Possuir filtro de aplicações de modo a permitir a identificação de padrões de dados dentro das conexões, possibilitando o tratamento automático (auditoria, geração e alertas, bloqueios e liberação) serviços bem como de aplicações do tipo peer-to-peer, de download de arquivos, entre outros;

4.2.201. Deverá permitir que as assinaturas de detecção e prevenção sejam associadas a grupos de servidores específicos;

4.2.202. Prover mecanismo contra ataques de falsificação de endereços (IP Spoofing) através da especificação da interface de rede pela qual uma comunicação deve se originar;

4.2.203. Prover proteção contra os ataques de negação de serviço SYN Flood, Land, Tear Drop e Ping O'Death;

4.2.204. Possuir mecanismo que limite o número máximo de conexões simultâneas de um mesmo cliente para um determinado serviço e/ou servidor;

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

4.2.206. Possuir sistema de prevenção de intrusão (IPS) nativo, permitindo o bloqueio do ataque em caso de detecção do mesmo;

4.2.207. Usar autenticação forte e mecanismos de criptografia para todos os componentes da solução;

4.2.208. Suportar novos protocolos sem a necessidade de alterar o hardware;

4.2.209. Remontar todos fluxos de pacote fragmentados ou não;

4.2.210. Permitir reinicialização do sensor sem interrupção de tráfego;

4.2.211. Deverá suportar o conceito de pré-processador, permitindo que um determinado protocolo funcione apenas em um conjunto de portas. Este conceito pode ser utilizado nos proxies que tem portas dinâmicas como: RPC, FTP, SIP, H323. Assim, as regras destes protocolos não seriam aplicadas em todas as portas e conexões, seriam aplicadas apenas nas conexões negociadas, economizando CPU;

4.2.212. Fabricante deve garantir o fornecimento de atualizações regulares dentro do período de assinatura contratado;

4.2.213. Deverá permitir a atualização automática das assinaturas por meio de agendamento diário ou de hora em hora;

4.2.214. Possuir mecanismo que permita fazer download apenas das novas atualizações das assinaturas diárias e não da base completa, de modo a economizar banda do link com a Internet;

4.2.215. Prover linguagem para criação de regras proprietária ou compatível com assinaturas do Snort;

4.2.216. Deve implementar proteção positiva e segura contra:

4.2.216.1. Ataques de Worm, Trojan, Backdoors, Portscans, IP Spoofing, DoS e Spywares;

4.2.216.2. Ataques a comunicações VoIP;

4.2.216.3. Ataques e utilização de tecnologia P2P;

4.2.216.4. Ataques de estouro de pilha (buffer overflow);

4.2.216.5. Ataques do tipo dia-zero (zero-day);

4.2.216.6. Tráfego mal formado;

4.2.216.7. Cabeçalhos inválidos de protocolo;

4.2.217. Deve possuir filtros de normalização de tráfego, que bloqueiem tráfego malicioso ou que apresente comportamento anormal. Deve possuir a capacidade de bloquear os seguintes tipos distintos:

4.2.217.1. IP Header Incomplete;

4.2.217.2. IP Fragment Invalid;

4.2.217.3. IP Fragment Out of Range;

4.2.217.4. IP Duplicate Fragment;

4.2.217.5. IP Length Invalid;

4.2.217.6. IP Fragment Total Length Mismatch;

4.2.217.7. IP Fragment Overlap;

4.2.217.8. IP Fragment Bad MF Bits;

4.2.217.9. IP Fragment Expired;

4.2.217.10. TCP Segment Overlap With Different Data;

4.2.217.11. TCP Header Length Invalid;

4.2.217.12. TCP Flags Invalid;

4.2.217.13. TCP Header Incomplete;

4.2.217.14. TCP Length Invalid;

4.2.217.15. TCP Reserved Flags Invalid;

4.2.217.16. ICMP Header Incomplete;

4.2.217.17. UDP Header Incomplete;

4.2.217.18. UDP Length Invalid;

4.2.217.19. Ethernet Header Incomplete;

4.2.217.20. ARP Address Invalid;

4.2.217.21. ARP Header Incomplete;

4.2.217.22. ARP Length Invalid;

4.2.217.23. DPI (Deep Package Inspection - DPI)

4.2.218. Possuir capacidade de inspeção profunda de pacotes (Deep Package Inspection - DPI), incluindo todo o payload;

4.2.219. Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos e transferências de arquivos do tipo P2P (peer to peer) tais como Kazaa e de IM (Instant Messaging), tais como ICQ, MSN;

4.2.220. Possuir a capacidade de controlar, bloquear o download de tipos de arquivos específicos via FTP e HTTP;

4.2.221. Permitir o controle de acesso por usuário e grupos para controle de IMs como Skype, Google Talk, Yahoo Messenger e Facebook Messenger;

4.2.222. Possuir a capacidade de identificar o tráfego Web e classifica-lo de acordo com as aplicações e sub aplicações trafegando na rede, tais como redes sociais: Facebook, Google+, Twitter, etc; de comunicação: Skype, Gmail, GTalk, MSN, etc;

4.2.223. Permitir 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 Ultrasurf, Skype e ataques mediante a porta 443;

4.2.224. Suportar a detecção de aplicações dinâmicas dentro de sessões de proxy HTTP;

4.2.225. Este serviço deve detectar e bloquear ao menos 3.300 (três mil e trezentas) assinaturas de aplicações;

4.2.226. Filtro de Acesso Web com Atualização De URL's para UTM

4.2.227. A base de conhecimento WEB, que irá executar dentro do próprio appliance sem a necessidade de utilização de outro servidor, deve ser fornecido, durante todo o contrato, com todas as atualizações de bases de URLs, categorias, software embarcado, e deverá conter as seguintes características:

4.2.228. Deverá fornecer filtro de acesso web conforme especificações a abaixo:

4.2.229. Possuir capacidade para efetuar classificação de URLs, de maneira a bloquear acesso a páginas WEB, para usuários ou grupo deles, a partir de categorias genéricas;

4.2.230. Possuir pelo menos 75 categorias de classificação de URLs a serem consultadas no analisador de URLs do item anterior;

4.2.231. Deverão ser fornecidas todas as atualizações de software assim como a atualização da base de conhecimento (URLs categorizadas), sem custo adicional, por todo o período do contrato;

4.2.232. Possibilitar agendamento mensal e semanal do download automático das atualizações das URLs;

4.2.233. Possuir mecanismo que permita fazer download apenas das novas atualizações diárias e não da base completa, de modo a economizar banda do link com a Internet;

4.2.234. Possuir pelo menos 20.000.000 (Vinte Milhões) de URLs classificadas;

4.2.235. A aplicação que irá executar dentro do próprio appliance sem a necessidade de utilização de outro servidor, deve ser fornecida, durante todo o contrato, com todas as atualizações de assinaturas, software embarcado, e deverá conter as seguintes características:

4.2.236. Deverá fornecer filtro de antivírus conforme especificações a abaixo:

4.2.237. Possuir verificação integrada de antivírus, de forma a poder verificar contra vírus todos os arquivos e/ou páginas web acessados ou baixados através dos protocolos HTTP, SMTP, IMAP e FTP em browser;

4.2.238. Deverão ser fornecidas todas as atualizações de software assim como a atualização da base de conhecimento (novas assinaturas e vacinas), sem custo adicional, por todo o período do contrato;

4.2.239. Deverá analisar os arquivos e verificar a presença de vírus. Na existência de um vírus, deverá tentar sua desinfecção. Caso não consiga, o arquivo deverá ser descartado;

4.2.240. Deverá permitir análise heurística de vírus, configurável pelo administrador;

4.2.241. Deverá possibilitar que o administrador configure de forma independente a detecção e bloqueio de pelo menos as seguintes ameaças digitais: spywares, jokes, dialers e ferramentas de hackers;

4.2.242. Deverá permitir a atualização automática da base de identificadores de vírus por meio de agendamento diário ou de hora em hora;

4.2.243. Deverá permitir a atualização sob demanda da base de assinaturas de vírus;

4.2.244. Deverá ser capaz de analisar arquivos compactados no mínimo nos seguintes formatos: ZIP, ARJ, LHA, Microsoft CAB, ZOO, ARC, LZOP, RAR, BZIP2 e TAR;

4.2.245. Deverá ser capaz de analisar arquivos executáveis compactados pelos programas UPX, AsPack, PEPack, Petite, Telock, FSG, Crunch e WWWPack32;

4.2.246. Deverá ser capaz de analisar arquivos compactados em até 20 níveis, mesmo com formatos diferentes;

4.2.247. Deverá ter proteção automática contra ataques do tipo “BZIP bomb” e similares;

4.2.248. Todas as assinaturas de Antivírus deverão estar salvas localmente e não será permitida a consulta de assinaturas na nuvem;

4.2.249. A aplicação que irá executar dentro do próprio appliance sem a necessidade de utilização de outro servidor, deve ser fornecido, durante todo o contrato, com todas as atualizações de assinaturas, software embarcado, e deverá conter as seguintes características:

4.2.250. Deverá fornecer filtro de detecção de spam bayseano;

4.2.251. Fornecimento de todas as atualizações de software assim como a atualização da base de

conhecimento (novas regras de detecção de SPAM) por todo período do contrato;

4.2.252. Deverá avaliar as mensagens e atribuir uma nota a cada uma delas, que corresponda à probabilidade de a mesma ser SPAM, variando de 0 a 100%;

4.2.253. As notas atribuídas às mensagens deverão ser calculadas utilizando-se bancos de dados com informações estatísticas obtidas de milhares de mensagens de e-mail, e produzidas através de análise bayesiana;

4.2.254. Os bancos de dados com informações estatísticas deverão poder ser atualizados diária e automaticamente, através de download via Internet;

4.2.255. Deverá possuir dois modos distintos de atribuição de notas para as mensagens: um que prioriza a detecção de SPAM e outro que reduz os falso-positivos;

4.2.256. Deverá possibilitar que os usuários realizem treinamento do banco de dados de mensagens informando, para cada mensagem recebida, se a mesma é ou não SPAM;

4.2.257. Permitir a criação de bases de dados de classificação distintas para cada usuário ou grupo de usuários, a fim de que cada base represente um perfil de usuário ou grupo de usuários específicos;

4.2.258. Permitir mecanismo que faça com que o treinamento de cada usuário seja aproveitado somente na base correspondente ao seu grupo ou usuário do sistema;

4.2.259. Permitir o backup e restauração das bases com os treinamentos dos usuários via interface de administração remota;

4.2.260. Deverá possuir plugins para realização do treinamento das mensagens pelo menos para os clientes de e-mail Microsoft Outlook e Thunderbird;

4.2.261. Deverá possuir mecanismo de treinamento de mensagens para os leitores de e-mail para os quais não exista plugin disponível, através da modificação da mensagem original. Esta modificação deverá funcionar para qualquer cliente de e-mail que suporte a leitura de mensagens HTML;

4.2.262. Possibilitar o registro de todas as classificações e treinamentos realizados através do servidor, e de todas as tentativas de abertura de sessões ou conexões que forem recusadas pelo mesmo;

4.2.263. Possibilitar o registro de todas as operações envolvendo as bases de dados do sistema de detecção, tais como download, upload e recálculo;

4.2.264. Possibilitar registro da remoção, restauração ou criação de backup de bases;

4.2.265. Possuir mecanismo que permita a configuração do log (tempo de permanência das mensagens, tamanho de arquivo, etc) e visualização das mensagens de log através da interface gráfica;

4.2.266. Possibilitar o envio de registros para o sistema operacional (syslog no caso de sistemas UNIX e Event Viewer em Windows);

4.3. Características gerais da solução integrada análise avançada de malware

4.3.1. Fornecimento de hardware e software para implantação de solução integrada de segurança, de mesmo fabricante, para proteção da rede de dados corporativos contra ciberataques avançados, direcionados e ameaças modernas de múltiplos vetores com solução centralizada de gerenciamento.

4.3.2. Todos os itens que compõem as especificações técnicas deverão ser de um mesmo fabricante;

4.3.3. A solução deverá prover as funcionalidades de inspeção de entrada (inbound) de malwares, com filtro de ameaças avançadas e análise de execução em tempo real (sandbox) de forma nativa on premises e inspeção de saída (outbound) de chamadas de retorno maliciosas (callbacks);

4.3.4. A solução deverá suportar um throughput mínimo de 1000 MBps, permitindo sua implementação em pelo menos 3 segmentos inline de forma nativa para inspeção on premises de ameaças oriundas do tráfego web;

4.3.5. A solução deverá ser entregue em formato virtualizado compatível com plataforma VMWare ESX obedecendo às seguintes características:

4.3.5.1. VMware EXSi versão 6.0 ou superior;

4.3.5.2. VMware vSphereClient;

4.3.5.3. Drivers de rede VMXNET3;

4.3.5.4. Link aggregation habilitado no ESXi;

4.3.5.5. Interfaces de rede suficientes para acomodar os sensores ;

4.3.6. A solução deverá ser entregue com todo o hardware e software necessário;

4.3.7. Não serão aceitos softwares personalizados, para o atendimento específico deste projeto, que sejam diferentes dos oferecidos pelo fabricante para o mercado em geral;

4.3.8. Especificação mínima do servidor virtual para execução da solução:

4.3.8.1. Possuir no mínimo 6 (seis) núcleos (cores);

4.3.8.2. Possuir no mínimo 16 (dezesseis) GB de memória RAM;

4.3.8.3. Possuir no mínimo 384 (trezentos e oitenta e quatro) GB de espaço em disco (HD);

4.3.8.4. Possuir no mínimo 02 (duas) interfaces 10/100/1000 Base-T para cada segmento de rede a ser monitorado;

4.3.8.5. Possuir no mínimo 01 (uma) porta de gerenciamento 10/100/1000 Base-T;

4.3.9. Prover em sua análise de sandbox local a identificação de novos destinos de callbacks oriundos de malwares zero-day e/ou exploits web, não dependendo de soluções terceiras ou módulos adicionais para retroalimentação da proteção;

4.3.10. Suportar o bloqueio de ataques exploit e malwares na entrada, ataques obfuscados, saída de callbacks multiprotocolo em formato inline;

4.3.11. Permitir categorização de atividades de riskware tais como adwares e spywares;

4.3.12. Ser capaz de prover inteligência contextual sobre um ataque ou atacante previamente catalogado;

4.3.13. Permitir recebimento de indicadores de terceiros no padrão STIX;

4.3.14. Possuir integração nativa com ferramenta de endpoint do mesmo fabricante para compartilhar informações de atividade maliciosa;

4.3.15. Utilizar hypervisor proprietário que não dependerá de assinatura, para execução de objetos web e binários suspeitos utilizando diferentes navegadores, aplicações e sistemas operacionais para rastrear

possíveis vulnerabilidades, corrupção de memória e outras ações maliciosas;

4.3.16. Suportar em seus perfis locais de Guest-Images nativos e ativos simultaneamente, pelos menos 3 diferentes imagens de Windows;

4.3.17. Suportar em seus perfis locais de Guest-Images nativos, pelos menos 2 diferentes versões de MacOS;

4.3.18. Durante a análise executada em tempo real, cada máquina virtual deverá suportar múltiplas versões de um mesmo aplicativo, como exemplo, mais de uma versão de Microsoft Office ou mais de uma versão de Adobe Reader em uma única máquina virtual;

4.3.19. Possuir rede de inteligência proprietária do fabricante, de forma a cobrir ataques originados de qualquer localidade global, com mecanismo opcional de retroalimentação de inteligência coletada localmente;

4.3.20. Permitir a detecção de exploração de vulnerabilidade mesmo sem o conhecimento ou identificação prévia da mesma;

4.3.21. Permitir a identificação e análise de todo o ciclo de vida de um ataque incluindo exploração de vulnerabilidade, download de binários, execução de malware e comunicação com o atacante em ambiente externo (callback);

4.3.22. Identificar e reportar técnicas de exploits responsáveis pela execução de código malicioso, em sua fase inicial de execução em memória, antes que ocorra o download do malware ofuscado.

4.3.23. Identificar ataques como: exploração zero-day, malwares polimorficos, vulnerabilidades desconhecidas e capturar e correlacionar todo ciclo do ataque

4.3.24. Possuir mecanismo para bloqueio inline nativo, não sendo aceito TCP-RESET ou HTTP Redirect como forma de bloqueio, ou ainda depender de módulos adicionais para o atendimento ao bloqueio.

4.3.25. Suportar em seus perfis locais de Guest-Images, sistemas operacionais Windows compatíveis com múltiplos idiomas incluindo árabe, russo, espanhol, chinês tradicional, chinês simplificado, francês, japonês, coreano e português no seu ambiente de sandbox local integrado para detecção de malwares;

4.3.26. Permitir a detecção de modificação de rotinas do Kernel;

4.3.27. Ser implementada in-line de modo totalmente transparente para o usuário final, sem a necessidade de instalação de agentes nos endpoints, configuração de proxies, rotas estáticas ou qualquer outro mecanismo de redirecionamento de tráfego;

4.3.28. Possuir a capacidade de executar download e atualização (instalação) das imagens de sistemas operacionais do ambiente de sandbox local integrado;

4.3.29. Suportar atualização da base de dados da Rede de Inteligência de forma automática e sem causar nenhum tipo de indisponibilidade da solução;

4.3.30. Permitir a análise de arquivos comprimidos com múltiplos níveis de compressão;

4.3.31. Permitir a identificação e exibição de alertas correlacionados, de ameaças que se utilizem de mais de um vetor de ataque;

4.3.32. Suportar headers XFF (X-Forwarded-For) para identificação das estações de trabalho;

4.3.33. Detectar e inspecionar, no mínimo, os seguintes tipos de arquivo, considerando as diferentes versões de sistemas operacionais e aplicativos existentes:

4.3.33.1. Documentos: doc, docx, xls, xlsx, ppt, pptx, ppsx, csv, rtf, vcf, vcs, pdf, eeml, eml, msg, xdp

4.3.33.2. Executáveis: bat, chm, cmd, com, dll, exe, msi, vbs

4.3.33.3. Web: html, htm,mht, url

4.3.33.4. Arquivo mídia: mp3, mp4, mov, midi, rm, rmi, qt, wav, wma, flv, swf, wsf, asf, 3gp, mpg, avi

4.3.33.5. Java/Javascript: jar, js

4.3.33.6. Imagem: jpg, png, ico, gif, tiff, jpeg

4.3.33.7. Arquivos: applet, hlp, hwp, hwt, lnk, xml

4.3.34. Exibir através de linha de comando, o status das submissões de malware realizadas no ambiente sandbox. Possibilitando a criação de filtros por:

4.3.34.1. IP de origem;

4.3.34.2. IP de destino;

4.3.34.3. MD5 do artefato;

4.3.35. Saber se a análise teve como veredicto ter sido considerada maliciosa ou não;

4.3.36. Todas as Guest-Images utilizadas na solução devem estar integralmente instaladas e ativadas nativamente pelo fornecedor;

4.3.37. Possuir tecnologia de hypervisor otimizado tanto para detecção de malwares avançados quanto para proteção contra ações de anti-debugging;

4.3.38. Prover análise automatizada contra malwares ou demais ameaças sem a necessidade de criação de regras ou políticas;

4.3.39. Prover verificação e análise de malwares e códigos maliciosos em tempo real sem verificações em cache engine ou batch mode;

4.3.40. Prover registro de toda a análise do comportamento da ameaça em tempo de execução, não sendo aceitas soluções baseadas em snapshot, estado de máquina virtual ou análises comparativas do tipo “antes e depois”;

4.3.41. Ser capaz de detectar e reportar cronologicamente quando APIs de sleep, checagem de hora do sistema, checagem de execução em VMware forem utilizadas por malwares em tentativas de evasão;

4.3.42. Suportar importação de regras YARA personalizadas, para permitir flexibilidade na criação de regras para análise de ameaças;

4.3.43. Suportar mecanismo de whitelist, permitindo a criação de regras por VLAN, subrede, endereço IP e Malware específico;

4.3.44. Ser capaz de funcionar em fail-open caso ocorra algum problema a nível de hardware, evitando impacto no ambiente de produção.

4.3.45. Ser administrada via console baseada em web, e que não seja necessário a instalação de software

adicional para sua gerencia;

4.3.46. Suportar interface gráfica WEB segura, utilizando o protocolo HTTPS e suportar instalação de certificado emitido por uma autoridade válida;

4.3.47. Suportar interface CLI segura através do protocolo SSH;

4.3.48. Possuir suporte IPMI;

4.3.49. Controlar acesso de usuários por nível, os quais podem ser atribuídos a usuários por perfil de privilégios;

4.3.50. Suportar gerenciamento das licenças de utilização da solução, incluindo adição e remoção de licenças;

4.3.51. Suportar base de usuários local e consulta a base de usuários externa através dos protocolos TACACS+ ou RADIUS ou LDAP;

4.3.52. Prover mecanismo automatizado através da interface web de administração para validação da correta implementação da solução, por meio da ativação de testes de download de malware e comunicação do tipo callback.

4.3.53. Suportar pela interface gráfica, seleção dos níveis e módulos de geração de log, tais como: log de autenticação de usuário, log de uso da Interface Gráfica, log da atividade relacionada ao hardware, log do mecanismo de checagem de saúde e log da base de dados;

4.3.54. Possuir mecanismos de backup da base de Dados e backup de configuração, via interface gráfica;

4.3.55. Suportar através da interface gráfica mecanismo para configuração de notificações dos alertas através de: e-mail ou SNMP;

4.3.56. Suportar integração com ferramentas de gerenciamento e correlação de logs suportando os formatos de evento: CEF, CSV , XML e LEEF;

4.3.57. Suportar através da interface gráfica mecanismo de atualização completa para todos componentes da solução

4.3.58. Suportar através da interface de administração, configuração de mecanismo de alerta onde seja possível configurar bloqueio/desbloqueio de uma comunicação do tipo callback;

4.3.59. Suportar IPv6;

4.3.60. Suportar mecanismo de integração com servidores Syslog nos modos TCP e UDP além de suportar também a alteração da porta de destino de Syslog padrão;

4.3.61. Suportar SNMPv3;

4.3.62. Suportar geração de relatórios através da interface gráfica onde contenha no mínimo as seguintes informações, com recursos de drilldown: tipo de malware, id de evento, extensão do arquivo inspecionado, severidade da ameaça, horário do último evento, ip de origem, ip de destino;

4.3.63. Suportar através da interface gráfica mecanismo de busca dos eventos arquivados através de palavras-chave;

4.3.64. Suportar através da interface gráfica ao menos os seguintes modelos de relatório: Sumário Executivo, Relatório de Servidores de Callback, Relatório de Hosts infectados, Atividade de Malware e detalhes dos alertas;

4.3.65. Suportar através da interface gráfica, a criação de filtros para apresentação dos alertas visualizados;

4.3.66. Suportar integração com ferramentas de gerenciamento e correlação de logs suportando os formatos de evento: CEF, CSV , XML e LEEF;

4.3.67. Prover dados forenses detalhados, via interface gráfica, relacionados ao ataque demonstrando seu o ciclo de vida completo. Estes dados forenses devem incluir a cronologia completa do ataque e não apenas uma porção do ataque, assim como:

4.3.68.Trilha completa de URLs, identificando todos os locais com os quais o malware tentou se comunicar:

4.3.68.1. Hashes MD5/SHA1,

4.3.68.2. Binários maliciosos anexados;

4.3.68.3. Mudanças no Sistema Operacional do Host;

4.3.68.4. Chaves de Registro, Sistemas de arquivo;

4.3.68.5. Sistema de inicialização;

4.3.68.6. Todas as chamadas de API que ocorreram;

4.3.69. Fornecer via interface gráfica capacidade de geração de PDF das principais telas de alertas;

4.3.70. Solução de oferta na modalidade Software como Serviço (SaaS) para combater ameaças modernas que se propagam através do vetor de e-mail;

4.3.71. Este serviço de subscrição endereça a necessidade de oferta de Segurança para e-mail baseado em Cloud, oferecendo proteção contra ameaças modernas e APTs;

4.3.72. A arquitetura da solução deverá ser capaz de realizar a correlação entre diferentes vetores de ataque.

4.3.73. Deverá prover rápida implementação através do modo de proteção ativo (Inline), configurado através do MTA de recepção, apontando diretamente para serviço em nuvem, ou apenas modo monitoramento através de regra utilizando cópia oculta (BCC);

4.3.74. Deverá prover "reforço" para segurança de domínio, de forma que seja compatível com configurações de SPF, DKIM e DMARC;

4.3.75. Deverá prover interface web para seu acesso e gerenciamento;

4.3.76. Deverá prover pelo menos 3 diferentes configurações de guest-image;

4.3.77. Deverá prover compatibilidade com RBAC, ou seja, regras de acesso baseado no perfil do usuário, para seu acesso e gerenciamento;

4.3.78. Deverá prover uma guia exclusiva para mensagens classificadas como "Ameaças Modernas";

4.3.79. Deverá prover bloqueio de ameaças em mais de 30 (trinta) diferentes tipos de arquivos anexados em e-mails e também URLs que possam conter exploits de dia-zero;

4.3.80. Deverá prover proteção para “one time URLs”, de forma que se verifique a reputação da URL em cada e-mail, adicionalmente ao processo de análise dinâmica;

4.3.81. Caso a URL seja considerada de má reputação, deverá ser apresentada uma página de bloqueio para o usuário final;

4.3.82. E-mails que contenham “URLs encurtadas” (ex: bit.ly) também deverão ser analisados em ambiente virtual dinâmico;

4.3.83. E-mails que estejam protegidos por senha, deverão ser verificados em ambiente virtual dinâmico, incluindo a possibilidade de configuração da lista de “senhas candidatas”;

4.3.84. Deverá prover relatório referente à análise do artefato ou URL, onde será possível:

4.3.85. Realizar download do pcap do tráfego;

4.3.86. Exibir em quais perfis de guest-image foi utilizada a análise onde a ameaça foi classificada como maliciosa;

4.3.87. Realizar o download do artefato, verificar o índice do VirusTotal para a ameaça e também exibir quais e quantas engines de Anti-Vírus consideram o artefato como malicioso;

4.3.88. Deverá prover relatório referente à análise do artefato ou URL, onde é possível: verificar de forma exclusiva, através de uma guia dedicada, o perfil de comunicação de rede para o artefato;

4.3.89. Deverá prover relatório referente à análise do artefato ou URL, onde é possível:

4.3.89.1. Verificar de forma clara, através de guia dedicada, todas as alterações que ocorreram a nível de Sistema Operacional: todas as chamadas de APIs, alterações ou criação de novos processos e chaves de registros, assim como alterações no UAC (user access control) e técnicas evasivas (chamadas sleep, injeções de código, consulta a relógio, etc.);

4.3.90. Deverá prover através de uma guia exclusiva, uma análise que correlaciona a Inteligência contra Ameaças, de forma que exiba qual nível do risco que a ameaça traz, se: Alto, Médio ou Baixo, assim como no mínimo os seguintes tipos de ameaças:

4.3.90.1. ATP;

4.3.90.2. Backdoor;

4.3.90.3. Downloader;

4.3.90.4. Exploit;

4.3.90.5. InfoStealer ;

4.3.91. Deverá prover, através de uma análise correlata com Inteligência contra Ameaças, a explicação da Atribuição da Ameaça, que tipo ou versão de software está vulnerável ao ataque, assim como o início da cadeia de Ataque (início do Kill Chain);

4.3.92. Deverá prover ações para mensagens quarentenadas, dentre as quais:

4.3.92.1. Liberar o E-mail;

4.3.92.2. Remover o E-mail;

4.3.92.3. Realizar o Download do E-mail;

4.3.93. Deverá prover configurações de políticas personalizadas baseadas em Domínios;

4.3.94. Deverá prover um e-mail de notificação para o usuário final, caso este seja alvo de mensagens com características de spear-phishing e adicionalmente permitir a configuração de ações para estas mensagens, entre as quais: liberar a mensagem;

4.3.95. Deverá oferecer o tracking da mensagem, mostrando seu veredicto: se foi quarentenada, ou liberada para entrega;

4.3.96. Deverá prover configuração para criar whitelists e blocklists baseados nos seguintes critérios:

4.3.96.1. Endereço de email do remetente;

4.3.96.2. Domínio do rementente;

4.3.96.3. MTP do remetente;

4.3.96.4. E-mail do recipiente;

4.3.96.5. URL;

4.3.96.6. MD5sum dos anexos;

4.3.97. Deverá ser capaz de correlacionar com a solução de gerencia centralizada, provendo dessa forma, uma correlação completa entre os vetores: Web e E-mail, e opcionalmente também Endpoint e Mobile;

4.3.98. Deverá prover classificação de mensagens que se utilizem de sites web, muito próximos, mas não iguais aos originais. Por exemplo: www.googlex.com em vez de: www.google.com;

4.3.99. Deverá ser capaz de "servir" binários fakes para artefatos que se utilizem de mecanismos de downloaders, e através disto, exibir o perfil de comunicação de call-back;

4.3.100. Deverá prover nível de serviço (SLA) de no mínimo de 99.99%;

4.3.101. Deverá prover compatibilidade com o padrão Yara 3.x e oferecer configuração de quanto de peso vale esta regra;

4.3.102. Deverá ser capaz de realizar análise estática;

4.3.103. Deverá prover proteção contra roubo de credencial através da análise de URL, análise de imagem e emulação HTML;

4.4. Características gerais da solução de gestão de senhas de alto-privilégio

4.4.1. Deverá prover armazenamento seguro e controle de credenciais não pessoais e privilegiadas em Servidores Linux/Unix, Windows (Incluindo contas de serviço como COM+ e IIS), Sistemas, Aplicações Web, Bancos de Dados, Estações de Trabalho e Dispositivos de Rede;

4.4.2. Prover autenticação transparente no sistema-alvo ou dispositivo de rede. A solução deve iniciar uma sessão injetando diretamente as credenciais na tela de login e servindo como um proxy para a sessão entre o usuário e o sistema-alvo, de forma que a senha não seja exposta ao solicitante do acesso;

4.4.3. Eliminar credenciais inseridas em códigos-fonte, scripts e arquivos de configuração, fazendo com que as senhas passem a ser gerenciadas pela solução e invisíveis aos desenvolvedores e equipe de

suporte de TI;

4.4.4. Gerar vídeos ou logs de textos das sessões realizadas através da solução, armazenados em repositório seguro, criptografado e protegido contra qualquer alteração que comprometa a integridade dessas evidências;

4.4.5. Ser composta por módulos de forma que seja possível montar um cofre de senhas da versão básica até a avançada, e com módulos adicionais compatíveis com os anteriores;

4.4.6. Fabricante sem compromisso com agências governamentais internacionais tais como NSA (National Security Agency) e ISA (Israel Security Agency).

4.4.7. A solução de hardware deve ser baseada em appliance e com sistema operacional customizado com banco de dados proprietário e embarcado, afim de garantir maior segurança e melhor desempenho da solução;

4.4.8. Possuir a quantidade de memória e capacidade de processamento listadas abaixo:

4.4.8.1. 2 Discos SATA 4T

4.4.8.2. RAM: 16GB

4.4.8.3. RAID 1: H330

4.4.8.4. Interfaces de Rede: 4

4.4.8.5. Interface de Gerenciamento Out-Of-Band

4.4.9. Possuir proteção contra ataque físico;

4.4.10. Possuir discos redundantes;

4.4.11. Possuir capacidade de armazenamento de chaves simétricas em hardware;

4.4.12. Possuir HSM embarcado;

4.4.13. Possuir módulo de TPM;

4.4.14. Possuir criptografia do disco;

4.4.15. Possuir redundância de disco;

4.4.16. Gabinete para instalação em rack padrão 19 polegadas, devendo cada equipamento possuir altura máxima de até 4U (unidade de rack);

4.4.17. Deve ser acompanhado de todos os cabos e suportes (gavetas, bandejas e braços) necessários para a instalação do equipamento em conformidade com as normas ABNT, quando se aplicar;

4.4.18. Fontes de alimentação redundantes e internas, hot-swappable, do tipo auto-sense, para operar de 100 a 240 VAC. Implementar redundância de fontes do tipo N + N, operando em frequência de 50/60Hz;

4.4.19. Implementar redundância de alimentação elétrica, com capacidade de substituição sem interrupção do funcionamento do equipamento (hot-swappable);

4.4.20. Possuir, pelo menos, 2 (duas) conexões independentes, permitindo a sua ligação a circuitos elétricos externos distintos;

4.4.21. Possibilidade de gerenciamento e utilização da solução através de interface Web;

4.4.22. Compatibilidade com, pelo menos, navegadores Google Chrome, Firefox e Internet Explorer;

4.4.23. Possibilidade de segregação de funções, baseado em perfis de acesso;

4.4.24. Permitir login dos usuários da solução utilizando dois fatores de autenticação;

4.4.25. Possibilidade de dois ou mais usuários solicitarem acesso a mesma conta privilegiada e/ou genérica, sem comprometimento da rastreabilidade;

4.4.26. Permitir aos administradores se autenticarem na interface de gerência da solução através de certificado digital;

4.4.27. Possuir módulo de gestão de certificados digitais;

4.4.28. A interface Web deve suportar a utilização de certificados digitais válidos pela ICP-Brasil e certificados auto-assinados gerados pela própria solução;

4.4.29. Operar como proxy de conexões via SSH/TELNET para qualquer dispositivo gerenciado, através de clients SSH como PuTTy, MobaXTerm, secureCRT e outros, sem a necessidade de abertura de um Terminal Service;

4.4.30. Prover conexões RDP controladas por meio do JUMP SERVER

4.4.31. Autenticar de forma confiável todas as requisições de senhas realizadas pela solução, com a finalidade de não permitir que qualquer usuário ou código malicioso tenha acesso ao repositório de senhas;

4.4.32. Toda a transmissão de dados entre os componentes da solução devem ser criptrografadas;

4.4.33. Sobre a utilização de padrões criptográficos por determinadas funcionalidades, a solução deve atender aos seguintes requisitos:

4.4.34. Utilizar algoritmo AES-256 para criptografia do tráfego de informações;

4.4.35. Para operações de autenticação e de acordo de chave de sessão, deve permitir a utilização de algoritmos dos sistemas de criptografia de chave pública RSA, Google Autenticator ou ECC;

4.4.36. Para os algoritmos do sistema de criptografia ECC, deve permitir a utilização de chaves;

4.4.37. Para os algoritmos do sistema de criptografia ECC, deve permitir a utilização de curvas Brainpool (RFC 5639);

4.4.38. Para os algoritmos do sistema de criptografia RSA, deve permitir a utilização de chaves;

4.4.39. Ser compatível com os seguintes sistemas/aplicações:

4.4.39.1. Sistemas Operacionais: Windows Server 2008 e superiores, Red Hat Enterprise Linux 6 ou superiores e AIX 61. E 7.1;

4.4.39.2. Aplicações Windows: Contas de serviço englobando contas de serviço do SQL server em cluster, tarefas agendadas, pools de conexão do IIS, COM+, usuário anônimo do IIS, serviços de Cluster;

4.4.39.3. Sistemas Gerenciadores de Banco de Dados: Oracle, Oracle RAC, MSSQL, MySQL;

4.4.39.4. Appliances de Segurança: CheckPoint, Nokia, Cisco, IBM, SourceFire e Imperva;

4.4.39.5. Dispositivos de redes: Cisco, D-Link, HP, 3com, Alcatel, Foundry, Brocade e ARUBA;

4.4.39.6. Aplicações: WebLogic, JBOSS, Tomcat, Peoplesoft, Oracle Application Server, Apache e IIS;

4.4.39.7. Serviços de Diretórios: OpenLDAP;

4.4.39.8. Acesso Remoto e monitoração: CA, IBM (Incluindo a HMC - Hardware Managemente Console dos servidores IBM), HP, iLO, Sun, Dell, DRAC, Digi, Cyclades, Fujitsu;

4.4.39.9. Ambientes Virtuais: Mware e Openstack;

4.4.39.10. Storages: Hitachi, EMC e IBM.

4.4.40. Possuir integração com HSM (Hardware Security Management) para aumentar a segurança física;

4.4.41. Integração nativa com soluções de SIEM/Syslog ;

4.4.42. Possibilidade de integração com ferramentas de Gestão de Mudanças;

4.4.43. Possuir workflow de aprovação para uso de credenciais;

4.4.44. Flexibilidade no processo de aprovação para o acesso a contas privilegiadas (acessos pré-aprovados, acessos com aprovação única, acessos com aprovação dupla ou outros que possam compor a solução);

4.4.45. Armazenamento e consulta de logs que forneçam ao menos, as seguintes informações:

4.4.46. Identificação do usuário que realizou determinado acesso a um dispositivo;

4.4.47. Identificação de quem aprovou o acesso do usuário;

4.4.48. Data e hora do acesso realizado e das ações que o usuário realizou no dispositivo remoto.

4.4.49. Prover, ao menos, os seguintes filtros para a recuperação de logs:

4.4.49.1. Usuário;

4.4.49.2. Sistema-alvo acessado

4.4.49.3. Tipo de atividade

4.4.49.4. Intervalo de tempo (data/hora/minuto inicial e final)

4.4.50. Deve vir acompanhado de todas as licenças de software ou hardware necessárias para atendimento das funcionalidades da solução;

4.4.51. Disponibilizar os Templates de troca de senha de forma que possam ser abertos, editáveis e auditáveis;

4.4.52. Não deverá depender de sistema operacional externo e/ou banco de dados que gerem a necessidade de licenças adicionais de outros fabricantes.

4.4.53. Não haver necessidade de utilização de ferramentas de terceiros para completar a solução, ou seja, um fabricante único que atenda todas as necessidades de um Cofre de Senhas;

4.4.54. Possibilidade de configuração em cluster de contingência, alta disponibilidade (HA) ou recuperação de desastres (DR);

4.4.55. Possibilidade de configuração do backup da solução e seus dados conforme Política de Backup da empresa.

4.4.56. Interface em Português do Brasil;

4.4.57. Aderente às Normas ISO/IEC 27.001, SOX e PCI.

4.4.58. Gerenciar todo o ambiente sem a necessidade de instalação de agentes ou qualquer software nos sistemas-alvos ou dispositivos de rede;

4.4.59. Geração automática de senhas de alta complexidade de acordo com as regras de cada tecnologia e Política de Segurança da empresa;

4.4.60. Realizar a troca automática das senhas, em horário programado, após terem sido liberadas para uso ou por vencimento de prazo;

4.4.61. Possibilidade de gerenciar senhas privilegiadas em aplicações e integração com sistemas legado;

4.4.62. Oferecer interface com visão personalizada exclusiva para Auditorias e Órgãos Reguladores, contendo os dispositivos e credenciais gerenciadas pela solução;

4.4.63. Prover área de transferência segura, de forma que o solicitante possa visualizar a senha ou copiá-la para a tela de login do sistema-alvo;

4.4.64. Liberação ou revogação de todos os acessos de uma determinada credencial de maneira automatizada e imediata;

4.4.65. Provisionamento de usuários locais em servidores Linux/Unix, Windows ou dispositivos de rede;

4.4.66. Notificar, via e-mail ou SMS, novas solicitações de aprovação de acesso aos respectivos responsáveis pelas credenciais;

4.4.67. Permitir o monitoramento on-line do uso das contas e desligamento da sessão;

4.4.68. Apresentar o recurso "break glass" para acesso de emergência às contas, ou seja, permitirá acesso a ativos protegidos de forma emergencial, sem a necessidade de aprovação prévia em contas no qual o usuário não teria acesso, sem perda de rastreabilidade;

4.4.69. Oferecer a funcionalidade de "Discovery" para realizar busca de novos servidores e elementos de rede, sendo capaz de levantar automaticamente as contas criadas nesses novos dispositivos;

4.4.70. Possibilidade de bloqueio e auditoria de comandos específicos;

4.4.71. Buscar por comandos específicos executados pelo usuário através de linha de comando em logs ou sessões gravadas;

4.4.72. Configuração de alertas imediatos quando realizados determinados comandos por usuários privilegiado;

4.4.73. Possibilidade de geração de relatórios baseados nos logs e exporta-los para arquivos em formato “.csv";

4.4.74. Extrair informações do servidor localizado nos Data Centers remotos caso seja necessário restaurar todas as configurações e os dados da solução de cofre de senhas;

4.4.75. Possuir mecanismo para exportar arquivo com as últimas senhas para repositório remoto, de forma criptografada e protegida por senha de dupla custódia para recuperações de senhas no caso de falha total da solução;

4.4.76. Possibilidade de arquitetura Ativo/Ativo sem a necessidade de um cluster externo à solução;

4.4.77. No caso de falha de um dos servidores do cluster de cofre de senhas de alta disponibilidade local, cada um dos servidores deve tratar todas as requisições de acesso, sem nenhum prejuízo no desempenho ou nas funcionalidades;

4.4.78. Alterações realizadas no cluster de cofre de senhas de alta disponibilidade local devem ser automaticamente replicadas para os outros servidores de redundância, de forma assíncrona e com delay máximo de 50ms;

4.4.79. Utilizar tecnologia de restrição e autenticação que inclua Assinatura Digital (Hash), Path e endereço IP do host ou conjunto de hosts a serem acessados pela solução;

4.4.80. Possibilidade de comunicação com os serviços de diretório via protocolo LDAPS;

4.4.81. Possibilidade de implementação SNMP sobre IPv6;

4.4.82. Implementar a especificação IETF RFC 2460, referente ao protocolo IPv6;

4.4.83. Possibilidade de implementar a MIB II, conforme RFC 1213;

4.4.84. Suportar sincronização do relógio interno via protocolo NTP e atualização automática do horário de verão com suporte e customização local.

4.5. Suporte Técnico / Implantação

4.5.1. Os serviços deverão ser obrigatoriamente executados pela CONTRATADA, ou por técnicos comprovadamente credenciados por esta, desde que as condições de operação atendam as exigências da mesma;

4.5.2. A avaliação inicial de toda solução será realizada pela CONTRATADA. Todas as etapas das configurações dos equipamentos deverão ser supervisionadas por equipe técnica da CONTRATANTE;

4.5.3. Configuração, Migração e Integração

4.5.3.1. O prazo de disponibilização do hardware e do licenciamento será no máximo de 30 (trinta) dias úteis, a contar da assinatura do contrato. Devendo-se considerar o menor tempo possível para troca dos atuais equipamentos em operação;

4.5.3.2. Todo o levantamento (análise de regras, rede, aplicações, serviços e ambiente atual tratados por esta solução) será disponibilizado imediatamente após a contratação para a CONTRATADA e transferido para os novos equipamentos;

4.5.3.3. A implantação, migração, configuração e integração deverão ser efetuadas de acordo com o plano de implantação antecipadamente elaborado pela **CONTRATANTE** em conjunto com a **CONTRATADA**, visando obter o melhor uso das soluções;

4.5.3.4. Toda e qualquer intervenção deverá ser planejada e programada de forma não haver interrupção no ambiente e serviços da **CONTRATANTE** ou que seja minima;

4.5.3.5. A contratada deverá efetuar a atualização, configuração, integração e testes de funcionalidade das soluções, buscando solucionar os eventuais problemas que possam ocorrer na **CONTRATANTE** e em terceiros que desta solução dependam;

4.5.3.6. A **CONTRATADA**, após concluídos os serviços de instalação, configuração, migração e integração deverá realizar junto aos técnicos da **CONTRATANTE**, testes de funcionalidade para constatar que os produtos foram implementados, configurados e integrados de acordo com os requisitos técnicos e parâmetros de configuração solicitados;

4.5.3.7. Concluídos os testes de funcionalidade, a contratada deverá elaborar uma documentação técnica (As Built), contendo todas as configurações efetuadas e as descrições das características e recursos utilizados a serem entregues a **CONTRATANTE**;

4.5.3.8. A **CONTRATANTE** providenciará as infraestruturas físicas (rack), elétricas e de rede de dados no local da instalação dos equipamentos;

4.5.3.9. A **CONTRATADA** deverá colocar à disposição da **CONTRATANTE**, analistas técnicos especializados para a execução do contrato, da solução e suas funcionalidades a serem implantadas, partindo dos itens básicos que seguem:

4.5.3.9.1. Planejamento da migração, implementações no ambiente, e terceiros;

4.5.3.9.2. Levantamento de políticas existentes utilizando-se de métodos e ou ferramentas visando-se uma migração das políticas de forma atualizada e limpa;

4.5.3.10. Integração com o Active Directory Corporativo e/ou outros serviços e recursos de TI necessários;

4.5.3.11. Configuração de políticas e novas funcionalidades, que permitam melhores resultados a Gestão de Segurança;

4.5.4. Configuração do IPS, VPN;

4.5.5. Configuração dos parâmetros de QoS que serão fornecidos pela equipe técnica da CONTRATANTE;

4.5.6. Testes e monitoração.

4.5.7. Monitoração Externa

4.5.7.1. Acompanhamento via Centro de Operações de Rede em regime 24 x 7 x 365;

4.5.7.2. A solução de monitoração desejada para este ambiente tem por objetivo identificar eventuais anomalias na operação de maneira precisa e em tempo real, melhorando o nível dos serviços prestados e consequentemente a satisfação dos usuários;

4.5.7.3. A prestação de serviços de monitoramento deverá contemplar:

4.5.7.3.1.Monitoração dos elementos constantes neste edital;

4.5.7.3.2. Treinamento na utilização das ferramentas disponibilizadas;

4.5.7.3.3. Manter o histórico analítico das monitorações pelo período contratual;

4.5.7.3.4. Enviar alertas através de e-mail e telefone quando alguma monitoração estiver indisponível ou com tempo de resposta fora do "threshold" (tempo mínimo e máximo de resposta), previamente definido, ou ainda quando houver detecção de ameaças. Para isto deverá ser estabelecida regra de acionamento para a **IOE**.

4.5.7.4. Característica Obrigatórias da Monitoração Externa

4.5.7.4.1. A solução deverá ter a capacidade de se integrar com softwares SIEMs de modo a enviar os seus logs para essas soluções;

4.5.7.4.2. A solução deverá ter a possibilidade de enviar logs para um SYSLOG SERVER;

4.5.7.4.3. A **CONTRATADA** deverá comprovar que seus processos asseguram backup e restauração dos dados monitorados com sigilo e confidencialidade das informações;

4.5.7.4.4. O registro de ocorrências deverá acontecer simultaneamente nas ferramentas de chamado da **IOE** e da **CONTRATADA**. A integração das ferramentas será responsabilidade da **CONTRATADA**.

4.5.7.4.5. Toda a Comunicação para a Supervisão, entre site da contratada e a **IOE**, deverá ser criptografada.

4.5.8. Serviços de Suporte Técnico de Segurança

4.5.8.1. A implantação e o suporte técnico continuado, com a avaliação de riscos, visa agregar no processo de tomada de decisões, referente à solução, ambientes e serviços correlacionais, através de competências específicas, utilizando-se de ferramentas, métodos e boas práticas de mercado;

4.5.8.2. Os chamados técnicos devem ser registrados por meio de email ou plataforma de abertura de chamados;

4.5.8.3. A equipe de supervisão do serviço deverá fazer o acompanhamento e abertura dos chamados, junto ao fabricante da solução, sempre que necessário;

4.5.8.4. Os processos de abertura de chamados por email ou telefone, devem ser baseados em padrões e boas práticas de serviços de Tecnologia da Informação. Devem assim garantir o fornecimento, no ato da abertura, de um número de chamado (protocolo) individual que possibilita a **CONTRATADA** acompanhar o andamento a qualquer momento;

4.5.8.5. Deve possuir no mínimo os processos para gestão de serviços, incidentes problemas e mudanças, baseado nas melhores práticas de Gerenciamento de Serviços de TI;

4.5.8.6. A **CONTRATADA** deve garantir que os equipamentos e meios utilizados pelos seus técnicos estejam livres de quaisquer programas ou características que possam causar danos à disponibilidade, confidencialidade ou integridade dos dados;

4.5.8.7. A **CONTRATADA** deve notificar à **CONTRATANTE** por meio de correio eletrônico sobre atualizações de softwares e hardware necessários para evitar problemas que possam ter um impacto negativo no ambiente de rede;

4.5.8.8. A **CONTRATANTE**, emitindo recomendações definitivas ou temporárias que evitem tais problemas, aplicando as correções recomendadas pelo fabricante do software ou hardware, após autorização da **CONTRATANTE**;

4.5.8.9. A **CONTRATADA** deverá apoiar no planejamento, atualização, implementação, ajustes, migração e a operação de novos projetos de mudança de topologia dos ativos de segurança contemplados neste edital;

4.5.8.10. A **CONTRATADA** deve executar as ações necessárias para apoiar os processos de resposta aos incidentes de segurança identificados, de forma a manter os serviços disponíveis e operacionais;

4.5.8.11. Serão considerados incidentes de segurança qualquer ação que vise comprometer a integridade, a confidencialidade das informações ou a disponibilidade dos serviços de tecnologia da informação da **CONTRATANTE**;

4.5.8.12. A **CONTRATADA** deve verificar e informar, regularmente, a disponibilização pelo fabricante da solução, de patches, correções e versões ou releases mais recentes dos softwares;

4.5.8.13. A C**ONTRATADA** deve validar o Gerenciamento de Operação e Segurança da solução, junto a **CONTRATANTE**, a fim de cumprir as melhores praticas na manutenção do ambiente: backup de configuração de sistemas (regras), aplicação de “Patches” e novas atualizações de software, gerenciamento de modificações e análise de logs, emitindo indicadores da solução com referência ao estado de segurança do ambiente;

4.5.8.14. A **CONTRATADA** deve prover suporte remoto sempre que solicitado e para solução em problemas considerados críticos e não solucionados pelos outros processos de suporte;

4.5.8.15. A **CONTRATADA** deve realizar ajuste fino (tunning) de toda a solução, adequando-a ao

ambiente e às customizações de configuração necessárias para atender às necessidades da **CONTRATANTE;**

4.5.8.16. A **CONTRATADA** deverá realizar periodicamente procedimentos ou atualizações necessárias para mitigar vulnerabilidades dos componentes da solução de segurança.

4.5.9. Gerência de Serviços

4.5.9.1. A **CONTRATADA** deve apresentar relatório mensal (gerencial) específico contendo, alertas, métricas, indicadores técnicos, indicadores de desempenho, níveis de serviço, requisições de serviços e incidentes em nível técnico. Estes devem ter a possibilidade de ser gerados no mínimo em PDF;

4.5.9.2. A contratada deverá realizar testes de verificação de qualidade e saúde da solução, sempre que solicitado, ou pró-ativamente em um prazo máximo de 3 meses, no total de 4 avaliações por contrato, sem custo adicional para realização do mesmo;

4.5.9.3. A **CONTRATADA** deve gerar relatórios pré-definidos ou sob demanda, em até cinco dias úteis à solicitação pela **CONTRATANTE**;

4.5.9.4. A **CONTRATADA** deve realizar rotinas de verificação dos sistemas e aplicações para emitir os relatórios de serviço, quando necessário;

4.5.9.5. A **CONTRATADA** deve propor a aplicação de melhores práticas às soluções de segurança existentes e melhorias nas topologias utilizadas pela CONTRATANTE quando necessário.

4.5.10. Gestão de Projeto

4.5.10.1. A contratada deverá informar nome, endereço, e-mail e celular dos componentes da equipe técnica responsável pela solução, ou seja, do gerente do projeto e do responsável comercial;

4.5.10.2. A **CONTRATADA** deverá manter atualizado meios de comunicação eficientes dos representantes aptos a interagir e resolver questões que excedam os canais de suporte;

4.5.10.3. No caso de inadequação técnica, a **CONTRATANTE** encaminhará à **CONTRATADA** os critérios e/ou mão de obra inadequados, encontrados nos serviços e solução, onde a contratada deverá avaliar em tempo, e após confirmação das inadequações, deverá ser agendada a efetivação

das devidas correções e/ou substituições;

4.5.11. Nível de Serviço

4.5.11.1. A **CONTRATADA** deve obedecer os seguintes níveis de serviço:

Incidente Tipo	SLA Tempo de resposta	Escalonamento
1	15 minutos	Intervalos de 15 minutos
2	20 minutos	Intervalos de 30 minutos
3	1 hora	Intervalos de 1 hora
4	6 horas	Intervalos de 8 horas

4.5.11.1.1. Incidentes **Tipo 1**: Indisponibilidade de uma função crítica causando impacto severo ou total indisponibilidade no fornecimento do serviço para todos os usuários e unidades de negócio, e não há alternativa ou "bypass" disponível.;

4.5.11.1.2. Incidentes **Tipo 2**: Uma aplicação, função ou sistema crítico está com desempenho deteriorado, impactando um grande número de usuários e com impacto nos negócios da **IOE**, havendo solução alternativa.;

4.5.11.1.3. Incidentes de **Tipo 3**: Uma função não crítica ou procedimento está inativo, não-utilizável ou difícil de ser usada, com algum impacto operacional, mas sem impacto imediato no fornecimento do serviço e existe alternativa ou "bypass" disponível;

4.5.11.1.4.Incidentes de **Tipo 4**: Significa que uma função não crítica ou procedimento está inativo, não-utilizável ou difícil de ser usada, mas sem impacto operacional, e existe alternativa ou "bypass" disponível;

4.5.11.1.5. Entende-se por início de atendimento, a hora de início de atendimento do técnico de suporte;

4.5.11.1.6. Entende-se por solução provisória (contorno), uma solução que minimize o impacto do problema mantendo a continuidade dos serviços;

4.5.11.1.7. Entende-se por término de atendimento, a disponibilidade da solução para uso em perfeitas condições de funcionamento no local onde está instalada.

4.5.12. Perfil das Atividades Técnicas/Operacionais

4.5.12.1. A CONTRATADA deve possuir e manter ao longo da vigência do contrato, profissionais qualificados e com experiência relacionada ao desenvolvimento das atividades propostas nesse Termo de Referência, como:

4.5.12.2. Metodologia e Sistema de Controle de Acesso;

4.5.12.3. Segurança em Telecomunicações, Redes e Internet;

4.5.12.4. Práticas de Gestão de Segurança;

4.5.12.5. Criptografia;

4.5.12.6. Arquitetura e Modelos de Segurança;

4.5.12.7. Requisitos básicos da informação (Confidencialidade, Integridade e Disponibilidade);

4.5.12.8. Risco, Resposta e Recuperação;

4.5.12.9. Medidas de redução do risco;

4.5.12.10. Tipos de ameaças, Atividades e códigos maliciosos;

4.5.12.11. Auditoria e Conformidade;

4.5.12.12. Tratamento de Incidentes de Segurança Computacional;

4.5.12.13. Boas práticas aplicadas a infraestrutura, operação e manutenção de serviços de tecnologia da

informação.

4.5.13. Assistência Técnica

4.5.13.1. O suporte técnico e atendimentos devem ser realizados em regime 24 x 7 x 365, em língua portuguesa.

4.5.14. **Vigência da Prestação dos Serviços**

4.5.14.1. Os serviços contratados deverão ser prestados por um período de 12 meses de forma contínua e ininterrupta, podendo, a critério da **IOE,** ser renovados por igual período até o limite permitido em lei;

5. QUALIFICAÇÃO E VISITA TÉCNICA

5.1. Relativamente à qualificação técnica, sem prejuízo das demais regras previstas no artigo 30 da Lei n.o 8.666/93, o licitante deverá apresentar comprovação de aptidão de desempenho de atividade pertinente, e indicação das instalações, do aparelhamento e do pessoal técnico adequados e disponíveis para a realização do objeto da licitação.

5.2. Capacitação técnico-operacional: Apresentação de atestado(s) fornecido(s) por pessoa(s) jurídica(s) de direito público ou privado, para a qual o licitante tenha executado serviços semelhantes ao objeto desta licitação.

5.3. Visando um perfeito entendimento das condições para prestação do serviço e elaboração da proposta comercial **é obrigatório** às empresas licitantes agendar uma visita técnica às instalações e recursos do ambiente de tecnologia da **IOE**, situado à Trav. do Chaco, 2271, bairro do Marco, Belém - PA, conforme o edital.

5.4. O agendamento poderá ser realizado através de contato com a **IOE** no telefone (**91**) **4009-7842**, e as visitas ocorrerão sempre nos dias úteis, em horário comercial, até 48 horas antes da abertura da licitação. As vistorias serão realizadas de acordo com os seguintes termos e condições:

5.4.1. A licitante poderá indicar um preposto para a realização da vistoria.

5.4.2. O representante da licitante deverá fornecer cópia autenticada de documento que comprove seu

vínculo com a licitante, ou procuração para realização da vistoria. Comprovação de que o proponente é devidamente um parceiro cadastrado e certificado pelo(s) fabricante(s) que os habilitem a prestar serviços descritos neste edital. Tais comprovações deverão ser feitas através de cópia dos certificados, carta do(s) fabricante(s) ou contrato de prestação de serviço com o proponente.

5.4.3. Ao final da vistoria será emitido **Termo de Vistoria** (**Apêndice I do Anexo II (Termo de Referência**) pelo representante da **IOE**, devidamente assinado pelo representante legal do licitante, comprovando que o licitante recebeu informações suficientes para elaboração de sua proposta de preços de forma clara, precisa e inequívoca, estando ciente de que não poderá alegar desconhecimento das condições de prestação de serviços.

5.5. Todos os custos diretos ou indiretos para realização das vistorias são de responsabilidade do licitante.

6. VALOR ESTIMADO DA CONTRATAÇÃO

6.1. As quantidades deverão obedecer às definições da tabela abaixo:

ITEM	DESCRIÇÃO	MÉTRICA	Qtd.	VALOR UNITÁRIO ESTIMADO	VALOR TOTAL ESTIMADO
1	Fornecimento de Firewall UTM composto por 01 Cluster com 02 (dois) appliances para ambiente de internet, com licenças de Antivirus, AntiSPAM, VPN, Web Filtering, IPS, Integração com o serviço de diretórios e LOG's.	Hardware	1	R$165.300,00	R$ 165.300,00
2	Licenciamento de serviço de plataforma de proteção de perímetro	Software	1	R$ 119.000,00	R$ 119.000,00

	(WAF – Web Application Firewall)				
3	Licenciamento de solução integrada anti-ransomware, tratando a segurança de rede e e-mail	Software	1	R$ 402.000,00	R$ 402.000,00
4	Licenciamento de software de gestão de Senhas de Alto Privilégio	Software	1	R$ 447.900,00	R$ 447.900,00
5	Prestação de serviços de avaliação técnica, implantação, configuração, migração e treinamento	Serviço	1	R$ 347.400,00	R$ 347.400,00
6	Prestação de serviços de monitoramento contínuo em regime 24x7x365, atualizações, suporte técnico e garantia	Serviço	12	R$ 63.200,00	R$ 758.400,00
VALOR TOTAL ESTIMADO				R$ 2.240.000,00	

7. SIGILO E CONFIDENCIALIDADE

7.1 A **CONTRATADA** deverá garantir a segurança das informações da IOE e se compromete a não divulgar ou fornecer a terceiros quaisquer dados e informações que tenha recebido da IOE no curso da prestação dos serviços, a menos que autorizado formalmente e por escrito para tal.

8. – DAS INFRAÇÕES E DAS SANÇÕES ADMINISTRATIVAS

8.7.1 Sem prejuízo das demais infrações previstas no presente termo de referência, comete infração administrativa, nos termos da Lei n.º 8.666, de 1993, da Lei n.º 10.520, de 2002, do Decreto n.º 3.555, de 2000, e do Decreto n.º 8.450, de 2005, a **CONTRATADA** que, no decorrer da contratação:
a) Inexecutar total ou parcialmente o contrato;
b) Apresentar documentação falsa;
c) Comportar-se de modo inidôneo;
d) Cometer fraude fiscal;
e) Descumprir qualquer dos deveres elencados no Edital ou no Contrato.
8.7.2 A **CONTRATADA** que cometer qualquer das infrações discriminadas no subitem acima ficará sujeita, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:
a) Advertência por faltas leves, assim entendidas como aquelas que não acarretarem prejuízos significativos ao objeto da contratação;
b) Multa:
b.1) Multa de 1,0 (um por cento) por dia de atraso incidente sobre o valor do faturamento, no todo ou em parte, e que será cobrado em dobro a partir do 31º (trigésimo primeiro) dia de atraso;
b.2) Multa de até 10% (dez por cento) sobre o valor total do Contrato, por infração de qualquer cláusula contratual, dobrável na reincidência;
c) Suspensão temporária de participar em licitação e impedimento de contratar com a Imprensa Oficial Estado, pelo prazo de até 02 (dois) anos;
d) 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.
e) A multa será aplicada sobre o valor do Contrato e será descontada dos pagamentos eventualmente devidos pela **CONTRATANTE** ou cobrada judicialmente.
8.7.3 A penalidade de multa pode ser aplicada cumulativamente com as demais sanções.
8.7.4 As penalidades serão obrigatoriamente registradas no SICAF.
8.7.5 As sanções aqui previstas são independentes entre si, podendo ser aplicadas isoladas ou, no caso das multas, cumulativamente, sem prejuízo de outras medidas cabíveis.
8.8 A desistência injustificada do lance ofertado ou, ainda que justificada, não aceita pelo pregoeiro e a não observância do prazo para assinatura do contrato, implicarão na inclusão da respectiva ocorrência junto ao SICAF, sem prejuízo das demais sanções previstas na Lei e no Edital:
a) Advertência – inciso I, art. 87 da Lei n.º 8.666/93;
b) Multa – art. 87, II da Lei n.º 8.666/93;
c) Suspensão Temporária – art. 87, III da Lei n.º 8.666/93;
d) Declaração de idoneidade – art. 87, IV da Lei n.º 8.666/93;
e) Impedimento de licitar e contratar com a administração pública – art. 7º da Lei n.º 10.520/02.

9. INTEGRAM ESTE TERMO DE REFERÊNCIA OS SEGUINTES ANEXOS:

9.1 Apêndice I – Modelo de Declaração de Vistoria

Aprovado, em ___ de _____ de _____.

ASS: _____

APÊNDICE I DO TERMO DE REFERÊNCIA - ANEXO II
PREGÃO ELETRÔNICO N.º 010/2017/IOE

MODELO DECLARAÇÃO DE VISITA TÉCNICA

DECLARO, para fins de participação no Pregão Eletrônico n.º 010/2017, que tomei conhecimento de todas as informações necessárias à execução de seu objeto, e que vistoriei os locais de instalação do software e componentes.

Belém, _____ de_____ de 2017.

_____

Carimbo e Assinatura do Responsável/Representante da Empresa

(Nome, cargo, CPF)

_____

Carimbo e Assinatura do Representante da IOE

ANEXO III DO PREGÃO ELETRÔNICO N.º 010/2017/IOE

MODELO DE PROPOSTA DE PREÇO

À

IMPRENSA OFICIAL DO ESTADO - IOE

Ref.: PREGÃO ELETRÔNICO N.º 010/2017

Prezados Senhores,

Após examinar todas as cláusulas e condições constantes do Edital em referência, apresentamos nossa proposta nos termos consignados no mencionado ato convocatório e seus anexos, com os quais concordamos plenamente.

O valor total de nossa proposta para o fornecimento de serviço de segurança da informação, fornecendo e integrando firewalls UTM, firewalls de aplicação WEB, gestão de senhas de alto-privilégio e proteção contra ameaças avançadas (ANTI-RANSOMWARE), incluindo pacote, administração de largura de banda (QoS), VPN, IPSec, SSL e IPS, antivírus, anti-spyware, para atendimento às características técnicas mínimas descritas no projeto, com o fornecimento de hardware, software e solução em nuvem, serviços de instalação, configuração, suporte, avaliação de ambientes, monitoramento contínuo, repasse tecnológico e migração das regras de firewall atualmente implementadas para as novas soluções, conforme especificações do Edital do PREGÃO ELETRÔNICO N.º 010/2017/IOE e seus anexos é de **R$ _____ (_____).**

ITEM	DESCRIÇÃO/MARCA	QUANT.	VALOR UNITÁRIO	VALOR TOTAL
01				

VALIDADE DA PROPOSTA	**60 (SESSENTA) DIAS.**
FORNECIMENTO DO OBJETO:	**PRAZO PARA ENTREGA E IMPLANTAÇÃO DO SISTEMA DE ACORODO COM O TERMO DE REFERÊNCIA (ANEXO II DO EDITAL).**
LOCAL DE ENTREGA:	**TRAVESSA DO CHACO, N.º 2271, BAIRRO: MARCO, CEP.: 66.093-542, BELÉM-PARÁ.**

OBSERVAÇÕES:	**OBSERVAÇÕES: (ESTE CAMPO É DESTINADO À INSERÇÃO DE TODOS OS DADOS COMPLEMENTARES À PROPOSTA QUE SE FIZEREM NECESSÁRIOS).** **OS PREÇOS PROPOSTOS ESTÃO INCLUÍDOS TODOS OS IMPOSTOS E TRIBUTOS, ENCARGOS SOCIAIS E FISCAIS, FRETE ATÉ O DESTINO (SEDE DA IOE), IMPLANTAÇÃO, TREINAMENTO, MANUTENÇÃO, SEGURO E QUAISQUER OUTROS ÔNUS QUE PORVENTURA POSSAM CAIR SOBRE O FORNECIMENTO DO OBJETO, OS QUAIS FICARÃO A CARGO, ÚNICA E EXCLUSIVAMENTE, DESTA PROPONENTE.**

Declaramos que estamos em Situação Regular perante a Fazenda Estadual, a Seguridade Social e Fundo de Garantia por Tempo de Serviço, atendendo também as exigências do presente Edital quanto à habilitação jurídica e qualificações técnica e econômico-financeira, bem como que não possuímos, no nosso quadro funcional, menores de dezoito anos, em trabalho noturno, perigoso ou insalubre, e nem menores de dezesseis anos em qualquer atividade, salvo como aprendiz, nos termos da Lei n.º 9.854/99, regulamentada pelo Decreto n.º 4.358, de 05/09/2002.

Caso nos seja adjudicado o objeto do Contrato, informamos que o Sr. _____ (nome completo), portador do CPF/MF n.º _____ e, da C.I. n.º _____, residente e domiciliado(a) na _____, n.º _____, bairro _____, CEP.: _____, é o(a) nosso(a) representante e está devidamente autorizado(a) e credenciado(a) a receber quaisquer comunicações relacionadas com o Instrumento Contratual, cujo pagamento deverá ser depositado no Banco _____, Agência _____, na Conta Corrente _____.

Atenciosamente,

PROPONENTE _____
Por _____
Cargo _____
Fone/Fax_____
E-mail_____

ANEXO IV DO PREGÃO ELETRÔNICO N.º 010/2017/IOE
MINUTA DO CONTRATO

CONTRATO N.º ...../2017/IOE DE ....., QUE ENTRE SI CELEBRAM A IMPRENSA OFICIAL DO ESTADO E A EMPRESA .....

Pelo presente Instrumento, **IMPRENSA OFICIAL DO ESTADO – IOE**, autarquia pública estadual, com personalidade jurídica de direito público interno, inscrita no CNPJ/MF sob o n.º 04.835.476/0001-01, com sede na Travessa do Chaco, n.º 2271, bairro: Marco, Belém-PA, CEP.: 66.093-542, neste ato representado por seu Presidente, Sr. **LUÍS CLÁUDIO ROCHA LIMA**, brasileiro, portador da Carteira de Identidade n.º ..... e do CPF/MF n.º ....., residente e domiciliado à ....., n.º ....., bairro ....., Belém-PA, CEP.: ....., doravante denominada simplesmente **CONTRATANTE** e, de outro lado, a empresa ....., CNPJ n.º ....., estabelecida na cidade de ..... (PA), sito à ....., n.º ....., Bairro ....., daqui por diante denominada simplesmente **CONTRATADA**, neste ato representada por ....., brasileiro(a), casado(a), portador (a) do CPF/MF n.º ..... e da Carteira de Identidade n.º ....., residente e domiciliado em ....., sito à ....., n.º ....., Bairro ....., CEP.: ....., têm entre si, justo e avençado e celebram, por força do presente instrumento, um Contrato de ..... que se regerá pelas disposições contidas neste instrumento e na melhor forma de direito, mediante as Cláusulas e Condições abaixo discriminadas e disposições legais, que voluntariamente aceitam e outorgam.

CLÁUSULA PRIMEIRA - DO OBJETO E AMPARO LEGAL

1.1 O objeto deste contrato é a aquisição de serviço de segurança da informação, fornecendo e integrando firewalls UTM, firewalls de aplicação WEB, gestão de senhas de alto-privilégio e proteção contra ameaças avançadas (ANTI-RANSOMWARE), incluindo pacote, administração de largura de banda (QoS), VPN, IPSec, SSL e IPS, antivírus, anti-spyware, para atendimento às características técnicas mínimas descritas no projeto, com o fornecimento de hardware, software e solução em nuvem, serviços de instalação, configuração, suporte, avaliação de ambientes, monitoramento contínuo, repasse tecnológico e migração das regras de firewall atualmente implementadas para as novas soluções, conforme condições estabelecidas no Edital, Termo de Referência e anexos do Pregão Eletrônico n.º 010/2017/IOE e tem como fundamento legal a Lei n.º 8.666, de 21/06/93, com as respectivas alterações

posteriores.

PARÁGRAFO ÚNICO – Aplicam-se ao presente instrumento, independentemente de transcrição, todas as especificações e condições previstas no Edital do Pregão Eletrônico n.º 010/2017/IOE, especialmente aquelas contidas no Termo de Referência, Anexo II, do referido instrumento.

CLÁUSULA SEGUNDA - DO PREÇO E DO VALOR TOTAL

2.1 Pelos serviços de fornecimento de licença perpétua do sistema objeto deste contrato, mediante o cumprimento de todas as condições previstas no Edital do Pregão Eletrônico n.º 010/2017/IOE e respectivos anexos, a **CONTRATANTE** pagará à **CONTRATADA** o valor total de **R$ XXXXX** (por extenso), não se admitindo qualquer reajuste sobre os valores originais propostos.
2.1. Pelos fornecimento do objeto deste contrato a **CONTRATANTE** pagará à **CONTRATADA** o valor mensal de **R$ XXXXX** (por extenso), como a seguir.
2.3. O Valor total do presente instrumento é de R$.....(.....)

ITEM	DESCRIÇÃO	QUANT.	VALOR UNITÁRIO	VALOR TOTAL
01				
02				
03				

2.4 No valor acima estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes do fornecimento do objeto, inclusive tributos e/ou impostos, encargos sociais, implantação, treinamento, manutenção, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação.

CLÁUSULA TERCEIRA - DAS CONDIÇÕES DE PAGAMENTO E REAJUSTE

3.1 O pagamento será efetuado pela CONTRATANTE, após a efetiva implantação do sistema, de acordo com as condições previstas no Edital e respectivos anexos, mediante processamento normal de liquidação, através da Diretoria Administrativa e Financeira da IOE, em até 30 (trinta) dias, mediante Ordem Bancária em conta corrente da CONTRATADA, em tudo obedecidos o Decreto Estadual n.º 877, de 31 de março de 2008 e Instrução Normativa n.º 0018, de 21 de maio de 2008 da Secretaria de Estado da fazenda – SEFA.
3.2 Pelos serviços de apoio e operação assistida do sistema, manutenção, suporte técnico e garantia, o pagamento será efetuado, mensalmente, após a efetiva comprovação da execução dos serviços, mediante o processamento normal de liquidação, através da Diretoria Administrativa e Financeira da IOE, em até 30 (trinta) dias, mediante Ordem Bancária em conta corrente da CONTRATADA, em tudo obedecidos o Decreto Estadual n.º 877, de 31 de março de 2008 e Instrução Normativa n.º 0018, de 21 de maio de 2008 da Secretaria de Estado da fazenda – SEFA.
3.2 Não haverá, sob hipótese alguma, pagamento antecipado à **CONTRATADA**.

3.3 Havendo erro na nota fiscal/fatura, ou circunstância que impeça a liquidação da despesa, aquela será devolvida à **CONTRATADA** e o pagamento ficará pendente até que seja sanado o problema ocorrido, o que deve ocorrer em até 30 (trinta) dias. Nesta hipótese, o prazo para pagamento se iniciará após a regularização da situação ou reapresentação do documento fiscal, não acarretando qualquer ônus para a **CONTRATANTE**.

3.4 O pagamento só será realizado após a comprovação da regularidade fiscal da **CONTRATADA**.

3.5 O pagamento somente será efetuado após o "atesto", pelo servidor competente, da Nota Fiscal/Fatura apresentada pela CONTRATADA.

3.6 O "atesto" fica condicionado à verificação da conformidade da Nota Fiscal/Fatura apresentada pela CONTRATADA e do regular cumprimento das obrigações assumidas.

3.7 Antes do pagamento, a CONTRATANTE realizará consulta *online* junto ao cadastro de fornecedores e, se necessário, aos sítios oficiais, para verificar a manutenção das condições de habilitação da CONTRATADA, devendo o resultado ser impresso, autenticado e juntado ao processo de pagamento.

3.8 Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

3.8.1 A CONTRATADA regularmente optante pelo Simples Nacional, instituído pelo artigo 12 da Lei Complementar n.º 123, de 2006, não sofrerá a retenção quanto aos impostos e contribuições abrangidos pelo referido regime, em relação às suas receitas próprias, desde que, a cada pagamento, apresente a declaração correspondente.

3.9 A CONTRATANTE não se responsabilizará por qualquer despesa que venha a ser efetuada pela CONTRATADA, que porventura não tenha sido acordada no contrato.

3.10 O preços dos serviços de manutenção contratados com prazo de vigência igual ou superior a doze meses será reajustado a cada interregno de 01 (um) ano, mediante a aplicação do índice setorial ou IGPM ou outro que venha substituí-lo.

3.11 O interregno mínimo de 01 (um) ano para o primeiro reajuste será contado a partir da data limite para apresentação das propostas constante do Edital.

3.12 Nos reajustes subsequentes ao primeiro, o interregno mínimo de 01 (um) ano será contado a partir da data de início da vigência do reajuste anterior.

3.13 Os reajustes, que não coincidirem com eventuais prorrogações de prazo, serão formalizados por meio de apostilamento.

CLÁUSULA QUARTA - DA VIGÊNCIA

4.1 O prazo de vigência do contrato será de **..... (.....) meses**, a partir da data da assinatura do instrumento, nos termos do artigo 57 da Lei n.º 8.666, de 1993.

CLÁUSULA QUINTA – DA DESPESA E DOS RECURSOS

5.1 A despesa decorrente da contratação do objeto desta licitação correrá à conta da seguinte:

Fonte de Recurso: 0661.00.0000
Natureza da Despesa: 3390.39
Programa de Trabalho – 22.131.1424.8233;
Plano Interno – 419.000.8233C.

Fonte de Recurso: 0261.00.0000
Natureza da Despesa: 3390.39
Programa de Trabalho: 22.131.1424.8233
Plano Interno – 419.000.8233C.

CLÁUSULA SEXTA - DAS OBRIGAÇÕES E RESPONSABILIDADES DAS PARTES

6.1 São obrigações e responsabilidades da CONTRATADA:

a) Efetuar a entrega do objeto no prazo e local indicados pela Administração, em estrita observância das especificações do Edital, Termo de Referência e proposta;

a.1) O objeto deve ser fornecido, quando for o caso, junto com o manual técnico do fabricante, com uma versão em português, relação da rede de assistência técnica autorizada, catálogos, folder, prospectos, fotos ou folheto;

a.2) Os bens deverão enquadrar-se, rigorosamente, dentro dos normativos da ABNT – Associação Brasileira de Normas Técnicas;

b) Executar o serviço de implantação nas dependências da IOE;

c) Responsabilizar-se pelos vícios e danos decorrentes do produto, de acordo com os artigos 12, 13, 18 e 26, do Código de Defesa do Consumidor (Lei n.º 8.078, de 1990);

c.1) Este dever implica na obrigação de, a critério da Administração, substituir, reparar, corrigir, remover, ou reconstruir, às suas expensas, no prazo máximo fixado no Termo de Referência, o produto com avarias ou defeitos;

d) Atender prontamente a quaisquer exigências da Administração, inerentes ao objeto da presente licitação;

e) Comunicar à Administração, no prazo máximo de 48 (quarenta e oito) horas que antecede a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação;

f) Manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

g) Não transferir a terceiros, por qualquer forma, nem mesmo parcialmente, as obrigações assumidas, nem subcontratar qualquer das prestações a que está obrigada, exceto nas condições autorizadas no Termo de Referência ou na minuta de contrato;

h) Não permitir a utilização de qualquer trabalho do menor de dezesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos; nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre;

i) Responsabilizar-se pelas despesas dos tributos, encargos trabalhistas, previdenciários, fiscais, comerciais, taxas, fretes, seguros, deslocamento de pessoal, implantação, treinamento, manutenção, prestação de garantia e quaisquer outras que incidam ou venham a incidir na execução do contrato;

j) Facilitar o acompanhamento e Fiscalização pela Imprensa Oficial do Estado do Pará, prestando prontamente, os esclarecimentos que forem solicitados pela **CONTRATANTE**;

k) Responder perante a **CONTRATANTE**, mesmo no caso de ausência ou omissão da Fiscalização, indenizando-a devidamente por quaisquer atos ou fatos lesivos aos seus interesses, que possam interferir na execução do contrato quer sejam eles praticados por empregados, prepostos ou mandatários seus;
l) Responder perante as leis vigentes, pelo sigilo dos documentos manuseados, sendo que a **CONTRATADA**, não poderá, mesmo após o término do contrato, sem consentimento prévio por escrito da **CONTRATANTE**, fazer uso de quaisquer documentos ou informações especificadas no parágrafo anterior, a não ser para fins de execução do contrato;
m) Responder, pecuniariamente, por todos os danos e/ou prejuízos que forem causados a União, Estado, Município ou terceiros, decorrentes da execução do objeto;
n) Manter durante toda a execução do objeto contratado, em compatibilidade com as obrigações por ele assumidas, todas as condições de habilitação e qualificação exigidas na licitação;
o) A **CONTRATADA** deverá manter durante a execução dos serviços os responsáveis técnicos e em caso de substituições, deverão ser comunicadas imediatamente a **CONTRATANTE**;
p) Substituir os profissionais somente nos casos de impedimentos fortuitos, de maneira que não prejudique o bom andamento da execução dos serviços;
q) A **CONTRATADA** deverá fornecer documento garantindo e comprovando que a licença do software aplicativo leitor, trata-se de uma licença perpétua.
r) A **CONTRATADA** deverá disponibilizar qualquer outro tipo de documentação referente ao software, que seja considerada importante pelo setor de informática da IOE/PA a qualquer momento que for requisitado do início ao fim do contrato;
s) A **CONTRATADA** deverá apresentar, por ocasião da assinatura do contrato, comprovação de que possui em seu quadro, profissionais qualificados para a execução dos serviços, objeto do contrato celebrado com a **CONTRATANTE**.

6.2 São obrigações e responsabilidades da **CONTRATANTE**:
a) Notificar, por escrito, à **CONTRATADA** acerca das irregularidades encontradas na entrega dos bens;
b) Efetuar o pagamento no prazo e condições estabelecidas;
c) Receber provisoriamente o material, disponibilizando local, data e horário;
d) Verificar minuciosamente, no prazo fixado, a conformidade dos bens recebidos provisoriamente com as especificações constantes do Edital e da proposta, para fins de aceitação e recebimento definitivos;
e) Acompanhar e fiscalizar o cumprimento das obrigações da **CONTRATADA**, através de servidor especialmente designado;

CLÁUSULA SÉTIMA – DA FISCALIZAÇÃO DO CONTRATO

7.1 A fiscalização da contratação será exercida por um representante da Administração, ao qual competirá dirimir as dúvidas que surgirem no curso da execução do contrato, e de tudo dará ciência à Administração.
7.2 O acompanhamento e a fiscalização da execução do contrato consistem na verificação da conformidade do fornecimento dos produtos, execução dos serviços e da alocação dos recursos

necessários, de forma a assegurar o perfeito cumprimento do contrato, e será exercido por servidor especialmente designado para esse fim atuando como Fiscal do Contrato, pela Imprensa Oficial do Estado - IOE, **na forma art. 67 da Lei n.º 8.666/93**, ficando a **CONTRATADA** obrigada a atender às observações de caráter técnico do fiscal, que se acha investido de plenos poderes para:
7.2.1 Conferir se o objeto entregue está de acordo com as especificações técnicas exigidas;
7.2.2 Informar à Diretoria Administrativa e Financeira da IOE, as ocorrências que exijam decisões e providências que ultrapassem a sua competência.
7.3 O representante da **CONTRATANTE** deverá ter a experiência necessária para o acompanhamento e controle da execução do contrato.
7.4 A fiscalização de que trata este item não exclui nem reduz a responsabilidade da fornecedora, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, ou emprego de material inadequado ou de qualidade inferior, e, na ocorrência desta, não implica em corresponsabilidade da Administração ou de seus agentes e prepostos, de conformidade com o art. 70 da Lei n.º 8.666, de 1993.
7.5 O fiscal do contrato anotará em registro próprio todas as ocorrências relacionadas com a execução do contrato, indicando dia, mês e ano, bem como o nome dos funcionários eventualmente envolvidos, determinando o que for necessário à regularização das faltas ou defeitos observados e encaminhando os apontamentos à autoridade competente para as providências cabíveis.

CLÁUSULA OITAVA – DO RECEBIMENTO DO OBJETO

8.1 O recebimento do objeto deste instrumento se dará em conformidade com o Termo de Referência (ANEXO II do Edital)
8.2 As obrigações resultantes do presente contrato deverão ser executadas fielmente pelas partes, de acordo com as condições avençadas e as normas legais pertinentes, respondendo cada uma delas pelas consequências de sua inexecução total ou parcial.

PARÁGRAFO ÚNICO – A Administração *rejeitará*, no todo ou em parte, os bens fornecidos ou serviços prestados em desacordo com o edital e seus anexos, através de termo circunstanciado, no qual deverá constar o motivo da não aceitação do objeto.

CLÁUSULA NONA - DAS SANÇÕES

9.1 Sem prejuízo de outras condutas definidas como infrações no Edital e seus anexos, comete infração administrativa, ainda, nos termos da Lei n.º 8.666, de 1993, da Lei n.º 10.520, de 2002, do Decreto n.º 3.555, de 2000, e do Decreto n.º 5.450, de 2005, a **CONTRATADA** que, no decorrer da contratação:
a) Inexecutar total ou parcialmente o contrato;
b) Apresentar documentação falsa;
c) Comportar-se de modo inidôneo;
d) Cometer fraude fiscal;
e) Descumprir qualquer dos deveres elencados no Edital ou no Contrato.
9.2 A **CONTRATADA** que cometer qualquer das infrações discriminadas no subitem acima ficará sujeita, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

a) Advertência por faltas leves, assim entendidas como aquelas que não acarretarem prejuízos significativos ao objeto da contratação;
b) Multa:
b.1) Multa de 1,0(um por cento) por dia de atraso incidente sobre o valor do faturamento, no todo ou em parte, e que será cobrado em dobro a partir do 31º (trigésimo primeiro) dia de atraso;
b.2) Multa de até 10% (dez por cento) sobre o valor total do Contrato, por infração de qualquer cláusula contratual, dobrável na reincidência;
c) Suspensão temporária de participar em licitação e impedimento de contratar com a Imprensa Oficial Estado, pelo prazo de até 02 (dois) anos;
d) 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.
e) A multa será aplicada sobre o valor do Contrato e será descontada dos pagamentos eventualmente devidos pela **CONTRATANTE** ou cobrada judicialmente.
9.3 A penalidade de multa pode ser aplicada cumulativamente com as demais sanções.
9.4 As penalidades serão obrigatoriamente registradas no SICAF.
9.5 As sanções aqui previstas são independentes entre si, podendo ser aplicadas isoladas ou, no caso das multas, cumulativamente, sem prejuízo de outras medidas cabíveis.
9.6 A desistência injustificada do lance ofertado ou, ainda que justificada, não aceita pelo pregoeiro e a não observância do prazo para assinatura do contrato, implicarão na inclusão da respectiva ocorrência junto ao SICAF, sem prejuízo das demais sanções previstas na Lei e no edital:
a) Advertência – inciso I, art. 87 da Lei n.º 8.666/93;
b) Multa – inciso II, art. 87 da Lei n.º 8.666/93;
c) Suspensão Temporária – inciso III, art. 87 da Lei n.º 8.666/93;
d) Declaração de idoneidade – inciso IV, art. 87 da Lei n.º 8.666/93;
e) Impedimento de licitar e contratar com a administração pública – art. 7º da Lei n.º 10.520/02.
PARÁGRAFO PRIMEIRO – Os valores das multas de que tratam os subitens anteriores deverão ser recolhidos a favor da **CONTRATANTE**, em conta a ser informada pela IOE, no prazo de até 5 (cinco) dias úteis, a partir da sua intimação por ofício, incidindo, após esse prazo, atualização monetária, com base no mesmo índice aplicável aos critérios do Governo Federal.

PARÁGRAFO SEGUNDO – Comprovado impedimento ou reconhecida força maior, devidamente justificado e aceito pela IOE, a **CONTRATADA** ficará isento (a) das penalidades mencionadas.

PARÁGRAFO TERCEIRO – As sanções de natureza pecuniária poderão, ainda, ser diretamente descontadas de créditos que eventualmente detenha a **CONTRATADA**.

CLÁUSULA DÉCIMA - DA RESCISÃO CONTRATUAL

10.1. O presente Termo de Contrato poderá ser rescindido nas hipóteses previstas no art. 78 da Lei nº 8.666, de 1993, com as consequências indicadas no art. 80 da mesma Lei, sem prejuízo da aplicação das sanções previstas no Termo de Referência, anexo do Edital.

10.2 Os casos de rescisão contratual serão formalmente motivados, assegurando-se à **CONTRATADA** o direito à prévia e ampla defesa.
10.3 A **CONTRATADA** reconhece os direitos da **CONTRATANTE** em caso de rescisão administrativa prevista no art. 77 da Lei n.º 8.666, de 1993.

CLÁUSULA DÉCIMA PRIMEIRA - DOS DIREITOS DO CONTRATANTE EM CASO DE RESCISÃO

11.1 Na hipótese de rescisão administrativa do presente contrato, a **CONTRATADA** reconhece, de logo, o direito da **CONTRATANTE** de adotar, no que couber, a seu exclusivo critério, as medidas que vão a seguir discriminadas:
a) Assunção imediata do objeto do contrato, no estado e local em que se encontrar, por ato próprio da **CONTRATANTE**;
b) Retenção dos créditos decorrentes do contrato até o limite dos prejuízos causados a **CONTRATANTE;**

PARÁGRAFO PRIMEIRO – Caso a **CONTRATADA** cometa falhas sucessivas ou demonstre desempenho insatisfatório na entrega dos produtos, à **CONTRATANTE** reserva-se o direito de notificar os demais licitantes observando-se a ordem de classificação final do certame, para adjudicação e homologação para o fornecimento dos produtos em questão. À **CONTRATADA** arcará com todas as despesas decorrentes.

PARÁGRAFO SEGUNDO – A utilização, pela **CONTRATANTE,** do direito a ela assegurada no item anterior, não implicará, necessariamente, em renúncia aos demais recursos postos à sua disposição por este contrato, não cabendo à **CONTRATADA** reivindicações de qualquer natureza em consequência da aplicação, pela **CONTRATANTE**, desta cláusula.

CLÁUSULA DÉCIMA SEGUNDA - DOS CASOS OMISSOS

12.1 Os casos omissos neste Termo de Contrato serão resolvidos à luz da Lei n.º 8.666/93 e suas alterações posteriores e dos princípios gerais de direito.

CLÁUSULA DÉCIMA TERCEIRA – DAS DISPOSIÇÕES FINAIS

13.1 As partes ficam, ainda, adstritas às seguintes disposições:
a) A **CONTRATADA** obriga-se a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado deste contrato;
b) Não será admitida, em nenhuma hipótese, a subcontratação objeto deste contrato; e
c) É vedado à **CONTRATADA** caucionar ou utilizar o presente contrato para qualquer operação financeira, sem prévia e expressa autorização da **CONTRATANTE**.

CLÁUSULA DÉCIMA QUARTA - DO FORO

14.1 Para a solução de quaisquer dúvidas, litígios ou questões outras decorrentes deste Contrato, fica declarado competente o Foro da Comarca de Belém, com a renúncia de qualquer outro, especial, privilegiado ou de eleição, que tenham ou venham a ter.

CLÁUSULA DÉCIMA QUINTA – DO REGISTRO E PUBLICAÇÃO

15.1 O presente contrato será publicado no Diário Oficial do Estado do Pará, sob a forma de extrato, e segundo os prazos estabelecidos, para que se cumpra com seus efeitos legais.

E por estarem justos e contratados, assinam o presente Contrato em 03 (três) vias, de igual teor e forma, na presença das testemunhas abaixo qualificadas, para que sejam produzidos os efeitos legais e jurídicos pretendidos.

Belém (PA), ... de ..... de 2017.

PELA CONTRATANTE: **LUÍS CLÁUDIO ROCHA LIMA**
PRESIDENTE DA IOE

PELA CONTRATADA:

TESTEMUNHAS:

1ª _____ **CPF:**_____

2ª _____ **CPF:**_____