EDITAL

PREGÃO ELETRÔNICO N° 007/2016

O BANCO DO ESTADO DO PARÁ S. A., por intermédio da Pregoeira designada pela Portaria n.º 155/2013 leva ao conhecimento dos interessados que, na forma da Lei Federal n.º 10.520/2002, Decreto Federal n.º 5.450/2005, Lei Estadual 6.474/2002, Decreto Estadual n.º 2.069/2006, Lei Complementar n.º 123/2006 e Decreto Estadual nº 878/2008 e subsidiariamente Lei n.º 8.666/1993 alterações posteriores, FARÁ REALIZAR LICITAÇÃO NA MODALIDADE PREGÃO, NA FORMA ELETRÔNICA, TIPO MENOR PREÇO, COM ADJUDICAÇÃO GLOBAL, COM OBSERVÂNCIA DAS CONDIÇÕES CONSTANTES DESTE EDITAL E SEUS ANEXOS.

Na data, horário e endereço eletrônico abaixo indicado far-se-á a abertura da sessão pública do Pregão Eletrônico, por meio de Sistema Eletrônico:

DATA: 11/02/2016
HORÁRIO DE BRASÍLIA: 11:00 HS
ENDEREÇO ELETRÔNICO: www.comprasnet.gov.br

Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a abertura do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subseqüente, no mesmo horário e local estabelecido no preâmbulo deste Edital, desde que não haja comunicação da Pregoeira em contrário.

1. DO OBJETO

1.1. O presente Pregão tem por objeto Contratação de empresa especializada no fornecimento de Solução Integrada de Serviços Gerenciados de Segurança Lógica, no modelo 24 horas por dia, 7 dias por semana, 365 dias por ano, inicialmente por 48 meses, incluindo o conjunto de hardware e software fornecidos em regime de comodato, necessários e suficientes para a prestação desses serviços, de acordo com o seguinte escopo:

- Serviço de Firewall Próxima Geração e VPN, para controle do tráfego nos segmentos protegidos;
- Serviço de Prevenção de Intrusos, para detecção e bloqueio de intrusão nos segmentos protegidos;
- Serviço de Gestão de Risco e Compliance, para descoberta e gestão de eventuais falhas de segurança no ambiente;

- Serviço de Gateway de E-mail e Web, para controle do tráfego de e-mail e proteção contra vírus, spam e conteúdo indesejado, assim como para controle do tráfego de internet e proteção contra vírus, acessos indevidos e conteúdo indesejado;
- Serviço de Proteção das Estações de Trabalho e Servidores de Rede (Tanto físicos, quanto virtuais) para identificar e mitigar infecções por vírus;
- Serviço de Proteção Contra Vazamento e Integridade dos Dados, para identificar e mitigar possíveis perdas de informações sensíveis;
- Serviço de Gestão de Eventos e Incidentes, para armazenagem, gerenciamento e correlacionamento de logs e eventos;
- Serviço de Proteção Contra Ameaças Dia Zero, para identificar e bloquear esse tipo de ameaça no ambiente da CONTRATANTE;
- Serviço de Monitoramento e Proteção de Base de Dados, para monitorar, identificar e controlar acesso aos bancos de dados;
- Disponibilização de banco de até 4.000 (mil) horas para a prestação de serviços técnicos, que possam ser utilizadas sob demanda.

Todas as especificações, exigências e obrigações estão estabelecidas no termo de referência, anexo I deste edital.

1.2. Havendo discordância entre as especificações deste objeto descritas no COMPRASNET-CATMAT e as especificações constantes do Anexo I – Termo de Referência, prevalecerão as últimas.

1.3. A adjudicação será GLOBAL.

1.4. NO CAMPO "DESCRIÇÃO DETALHADA DO OBJETO OFERTADO" DO SISTEMA COMPRASNET, OBRIGATORIAMENTE E SOB PENA DE DESCLASSIFICAÇÃO, O LICITANTE DEVERÁ DESCREVER A SÍNTESE DO OBJETO OFERTADO, NÃO SENDO ACEITÁVEL COMO DESCRIÇÃO APENAS O USO DA EXPRESSÃO "CONFORME O EDITAL" OU SIMILARES, SOB PENA DE DESCLASSIFICAÇÃO.

1.5. FICA VEDADO AO LICITANTE QUALQUER TIPO DE IDENTIFICAÇÃO QUANDO DO REGISTRO DE SUA PROPOSTA DE PREÇOS NO SISTEMA COMPRASNET, INCLUSIVE SENDO VEDADO INDICAR MARCA E FABRICANTE NO CAMPO "DESCRIÇÃO DETALHADA DO OBJETO OFERTADO", SOB PENA DE

DESCLASSIFICAÇÃO DO CERTAME. A MARCA E O FABRICANTE DEVEM SER INDICADOS EM CAMPO PRÓPRIO NO SISTEMA COMPRASNET.

2. CONSTITUEM ANEXOS DO EDITAL E DELE FAZEM PARTE INTEGRANTE

Anexo I: Termo de Referência
Anexo I-A: Declaração de visita técnica
Anexo II: Modelo de proposta de preços
Anexo II-A: Modelo de Declaração de Elaboração Independente de Proposta
Anexo III: Ordem de Serviço de Treinamento
Anexo IV: Termo de Recebimento de Serviços de Treinamento
Anexo V: Ordem de Serviço
Anexo VI: Termo de Confidencialidade, Zelo e Responsabilidade sobre os Bens de Informação do Banpará
Anexo VII: Modelo de Declaração de Inexistência de fato Impeditivo à Habilitação
Anexo VIII: Modelo de Declaração de não empregar menor
Anexo IX: Orçamento Estimativo
Anexo X: Minuta do Contrato (Anexo I do Contrato – Edital e Anexos e Proposta de Preços)

3. DA IMPUGNAÇÃO AO EDITAL

3.1. Até 02 (dois) dias úteis antes da data fixada para abertura da sessão pública, qualquer pessoa poderá impugnar o ato convocatório do Pregão Eletrônico, exclusivamente por meio eletrônico (via internet), enviando a impugnação para o e-mail **cpl@banparanet.com.br** até 16h.

3.2. Caberá à Pregoeira, auxiliada pelo setor responsável pela elaboração do Edital, decidir sobre a petição no prazo de até 24 (vinte e quatro) horas antes da abertura da sessão.

3.3. Acolhida a impugnação contra o ato convocatório, desde que altere a formulação da proposta de preços, será definida e publicada nova data para realização do certame.

3.4. As impugnações protocoladas intempestivamente serão desconsideradas.

4. DA SOLICITAÇÃO DE INFORMAÇÕES

4.1. Os pedidos de esclarecimentos referentes ao processo licitatório deverão ser enviados à Pregoeira, até 03 (três) dias úteis anteriores à data fixada para abertura da sessão pública, exclusivamente por meio eletrônico (via internet), no e-mail **cpl@banparanet.com.br até às 16h.** As informações e/ou esclarecimentos serão prestados pela Pregoeira através do site

www.banpara.b.br, ficando todos os licitantes obrigados a acessá-lo para obtenção das informações prestadas pela Pregoeira.

5. DAS CONDIÇÕES PARA PARTICIPAÇÃO

5.1. Poderão participar deste PREGÃO ELETRÔNICO os interessados que:

5.1.1. Desempenhem atividade pertinente e compatível com o objeto desta Licitação;

5.1.2. Atendam às condições deste EDITAL e seus Anexos, inclusive quanto à documentação exigida para habilitação, constante do item 12 deste Edital;

5.1.3. Estejam registradas no Sistema de Cadastramento Unificado de Fornecedores – SICAF, nos termos do §1º do art. 1º do Decreto 3.722, de 09.01.2001, publicado no D.O.U. de 10.01.2001;

5.1.3.1. As empresas não cadastradas no SICAF, e que tiverem interesse em participar do presente Pregão, deverão providenciar o seu cadastramento e sua habilitação junto a qualquer Unidade Cadastradora dos órgãos da Administração Pública, até o terceiro dia útil anterior a data de recebimento das Propostas (§ único, do art. 3º do Decreto 3.722/01).

5.1.3.2. As empresas estrangeiras deverão solicitar o seu credenciamento diretamente no COMPRASNET, até 03 (três) dias úteis antes da abertura da sessão.

5.1.3.2.1. A empresa estrangeira que não funcionar no Brasil, deverá apresentar os documentos estabelecidos no item 12 (Habilitação) do presente Edital, bem como o decreto ou Ato de autorização para o seu funcionamento no Brasil, já que a execução do objeto do contrato ocorrerá no Brasil (nos termos estabelecidos no art. 28, V e art. 32, §4º da Lei nº. 8.666).

5.1.3.2.2. No caso de inexistência de documentos equivalentes ou proibição ou dispensa por Lei ou Norma Legal, de apresentar quaisquer dos documentos solicitados no item 12 do Edital, o fato deverá ser devidamente declarado e comprovado, sob as penalidades da Lei Brasileira, sendo que os documentos que não estiverem redigidos em português (Brasil) somente serão aceitos se devidamente acompanhados das respectivas traduções por tradutor juramentado do Brasil.

5.2 Como requisito para participação no PREGÃO ELETRÔNICO o Licitante deverá manifestar, em campo próprio do Sistema Eletrônico, que cumpre plenamente os requisitos de habilitação e que sua proposta de preços está em conformidade com as exigências do instrumento convocatório, bem como a descritiva técnica constante do Termo de Referência no Anexo I do presente Edital.

5.3. Não poderão concorrer direta ou indiretamente nesta licitação:

5.3.1. Servidor de qualquer Órgão ou Entidade vinculada ao Órgão promotor da licitação, bem assim a empresa da qual tal servidor seja sócio, dirigente ou responsável técnico;

5.3.2. Consórcio de empresas, qualquer que seja a sua forma de constituição; grupos de empresas ou mais de uma empresa do mesmo grupo;

5.3.3. Empresa declarada Inidônea para licitar ou contratar com a Administração Pública, ou ainda, punida com Suspensão Temporária para licitar ou contratar, nos termos do art. 87, III e IV da Lei n.º 8.666/93. Referida Suspensão Temporária aplica-se no caso da empresa estar impedida/suspensa de licitar com o Banpará e/ou com o Estado do Pará e/ou Secretaria de Estado a qual o Banpará esteja vinculado;

5.3.4. Empresa que se encontre sob falência ou recuperação judicial ou extrajudicial, consórcios de empresas e que estejam coligadas ou subsidiárias entre si;

5.3.5. Empresas que tenham sido descredenciadas no Sistema Unificado de Cadastramento de Fornecedores – SICAF.

5.3.6. Membros da Diretoria Executiva, do Conselho Fiscal, do Conselho de Administração, Gerentes, funcionários e demais Administradores do órgão licitador.

6. DO CREDENCIAMENTO E DA REPRESENTAÇÃO

6.1. As empresas interessadas deverão proceder ao credenciamento antes da data marcada para início da sessão pública via Internet.

6.2. O credenciamento dar-se-á pela atribuição de chave de identificação e de senha, pessoal e intransferível, para acesso ao Sistema Eletrônico, no site **www.comprasnet.gov.br.**

6.3. O credenciamento e a sua manutenção requerem registro atualizado no Sistema de Cadastramento Unificado de Fornecedores (SICAF), que, também, será requisito para fins de habilitação, consoante o estabelecido no inciso I do art. 13 do Decreto Federal n.º 5.450/05 e inc. I do art. 14 do Decreto Estadual n.º 2.069/2006;

6.4. O credenciamento junto ao provedor do Sistema implica na responsabilidade legal única e exclusiva do licitante ou de seu representante legal e na presunção de sua capacidade técnica para realização das transações inerentes ao Pregão Eletrônico.

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

6.6. A perda da senha ou a detecção de indícios que sugiram a quebra de sigilo devem ser imediatamente comunicadas ao provedor do sistema, com vistas à adoção das medidas cabíveis e imediato bloqueio de acesso.

7. DA PROPOSTA DE PREÇOS

7.1. A participação no pregão eletrônico dar-se-á por meio da digitação da senha privativa do licitante e subseqüente encaminhamento da proposta de preços com valor cotado, a partir da data da liberação do edital no site **www.comprasnet.gov.br**, **até o horário limite de início da sessão pública, ou seja, até às 11h do dia 11/02/2016**, horário de Brasília, exclusivamente por meio do sistema eletrônico. Quando, então, encerrar-se-á, automaticamente, a fase de recebimento da proposta de preços. Durante este período o licitante poderá incluir ou excluir proposta de preços.

7.1.1. As microempresas ou empresas de pequeno porte deverão por ocasião do envio da proposta, declarar, em campo próprio do sistema, sob as penas da Lei, que atende os requisitos do art. 3º da Lei Complementar nº 123/2006, estando apta a usufruir do tratamento favorecido previsto na referida lei, conforme dispõe o art. 11 do Decreto Estadual Nº 878/2008.

7.2. Como requisito para a participação no Pregão o licitante deverá declarar, em campo próprio do sistema eletrônico, o pleno conhecimento e atendimento às exigências de habilitação previstas neste Edital.

7.3. FICA VEDADO AO LICITANTE QUALQUER TIPO DE IDENTIFICAÇÃO QUANDO DO REGISTRO DE SUA PROPOSTA DE PREÇOS NO SISTEMA COMPRASNET, SOB PENA DE DESCLASSIFICAÇÃO DO CERTAME, CONFORME ITENS 1.4 E 1.5 DESTE EDITAL.

7.4. O licitante será responsável por todas as transações que forem efetuadas em seu nome no sistema eletrônico, assumindo como firmes e verdadeiras suas propostas e lances, de acordo com o previsto no inciso III, art. 13, do Decreto Federal n.º 5.450/05 e inc. III do art. 14 do Decreto Estadual n.º 2.069/2006;

7.5. Incumbirá ainda 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, conforme disposto no inciso IV, art. 13, do Decreto Federal n.º 5.450/05 e inc. IV do art. 14 do Decreto Estadual n.º 2.069/2006;

7.6. O licitante deverá obedecer rigorosamente aos termos deste Edital e seus anexos. E em caso de discordância existente entre as especificações deste objeto descritas no COMPRASNET - CATMAT e as especificações constantes do Anexo I - Termo de Referência deste Edital prevalecerão às últimas.

7.7. Na proposta de preços, a ser enviada pelo licitante que cotou o menor preço, deverão constar, pelo menos, as seguintes condições, **conforme modelo constante do Anexo II deste edital com observância ao Termo de Referência, Anexo I e demais anexos do edital :**

a) 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;

b) Prazo de validade de no mínimo **120 (cento e vinte) dias consecutivos**, a contar da data de sua apresentação.

c) Preço global (unitário e total) de acordo com o(s) preço(s) praticado(s) no mercado, conforme estabelece o inciso IV do art. 43 da Lei Federal nº. 8.666/93 e conforme modelo de proposta**,** contido no **Anexo II do edital**. Os valores devem constar em algarismo e por extenso (total), expresso em moeda corrente nacional (R$), com no máximo 02 (duas) casas decimais, INCLUSIVE NA ETAPA DE LANCES, considerando a prestação do serviço constante no Termo de Referência - Anexo I do presente Edital. **(para a composição do valor global da proposta, observar o modelo de proposta de preços do anexo II do edital).**

c.1) NÃO SE ADMITIRÁ PREÇO GLOBAL OU UNITÁRIOS SUPERIORES AO ORÇAMENTO ESTIMADO.

d) Declaração de que está de pleno acordo com todas as condições, exigências e obrigações estabelecidas no Edital e seus Anexos, bem como que aceita todas as obrigações e responsabilidades especificadas no edital e seus anexos, em especial, no termo de referência e instrumento de contrato;

e) Apresentar declaração independente de proposta, nos termos do modelo constante do **Anexo II-A.**

7.8. Todas as características técnicas exigidas na especificação das soluções técnicas deverão ser comprovadas, independente da descrição da proposta, através de documentos cujas origens sejam exclusivamente o fabricante dos equipamentos, como CATÁLOGOS, MANUAIS, FICHA DE ESPECIFICAÇÃO TÉCNICA OU PÁGINAS OBTIDAS NO SITE OFICIAL DOS FABRICANTES, SOB A FORMA DE VOLUMES IMPRESSOS OU EM MEIO ELETRÔNICO (CD, DVD, ETC.);

7.8.1. As informações obtidas em sites oficiais do fabricante através da Internet deverão ser impressas e anexadas à proposta e deverá ser indicado à respectiva URL (uniform Resource Locator) onde se encontram;

7.8.2. Serão aceitos documentos em português ou inglês para comprovações técnicas;

7.8.3. A equipe técnica do BANPARÁ poderá realizar pesquisas adicionais para corroborar o atendimento, ou não, das características técnicas exigidas na especificação das soluções técnicas, caso a documentação apresentada seja insuficiente ou deixe dúvidas;

7.8.4. A não comprovação de alguma característica exigida levará a desclassificação da proponente.

7.9. No preço apresentado pela licitante já estão incluídos todos os tributos e demais encargos que incidam ou venham a incidir sobre o Contrato e a execução dos serviços referidos, assim como contribuições previdenciárias, fiscais e parafiscais, PIS/PASEP, FGTS, IRRF, emolumentos, seguro de acidente de trabalho, transportes e outros, ficando excluída qualquer solidariedade do Banpará, por eventuais autuações.

7.10. Quaisquer tributos, custos e despesas diretos ou indiretos omitidos da proposta ou incorretamente cotados serão considerados como inclusos nos preços, não sendo considerados pleitos de acréscimos.

7.10.1. O BANPARÁ não aceitará qualquer cobrança posterior de quaisquer encargos financeiros adicionais, salvo se criados após a data de abertura desta licitação e que venha, expressamente incidir sobre seu objeto na forma da lei.

7.11. O licitante será responsável pelas transações efetuadas em seu nome, assumindo como firmes e verdadeiras suas propostas e lances, inclusive os atos praticados diretamente ou por seu representante, não cabendo ao provedor do sistema ou ao órgão promotor da licitação responsabilidade por eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros. (inciso III do art. 13 do Decreto Federal n.º 5.450/05 e inc. III do art. 14 do Decreto Estadual n.º 2.069/2006).

7.12. Caso exista algum fato que impeça a participação de quaisquer licitantes, ou o mesmo tenha sido declarado inidôneo para licitar ou contratar com a administração pública, este fica impedido de participar da presente licitação, correspondendo a simples apresentação da proposta a indicação, por parte do licitante, de que inexistem fatos que impeçam a sua participação na presente licitação, eximindo assim a Pregoeira do disposto no art. 97 da Lei nº 8.666/93.

7.13. A Pregoeira verificará as propostas de preços enviadas, antes da abertura da fase de lances, desclassificando, motivadamente, aquelas que de pronto, não atenderem às exigências do presente Edital e seus Anexos, sejam omissas ou apresentem irregularidades insanáveis, ou defeitos capazes de dificultar o julgamento.

7.14. A apresentação da proposta implicará a plena aceitação, por parte do licitante, das condições estabelecidas.

8 - DA VISITA TÉCNICA OBRIGATÓRIA

8.1. Para que a empresa licitante compreenda a complexidade do ambiente tecnológico do BANPARÁ, as Empresas **deverão** visitar as instalações do BANPARÁ, **situado na Rua Municipalidade, 1036, Umarizal – 66.050-350 e Av. Presidente Vargas, 251, Centro – 66.010-000, ambos localizados – Belém-Pará,** conjuntamente com funcionário responsável pela licitação, para dirimir quaisquer dúvidas que se fizerem necessárias.

8.2. A Visita técnica deverá ser realizada por um representante legal da empresa LICITANTE ou por seu procurador, devidamente autorizado através de procuração;

8.3. A comprovação da visita técnica deverá ser através de uma declaração emitida pelo próprio licitante (modelo no anexo I-A) de que está de acordo com a realização dos serviços, não tendo nenhuma dúvida que venha a modificar ou prejudicar os quantitativos e especificações indicadas no Termo de Referência.

8.4. A visita técnica poderá ser realizada no período de 27/01/2016 a 01/02/2016, deve ser agendada pelos telefones: (091)3348 3620 – 9 9902 2981 SÉRGIO FONTOURA JUNIOR, (091) 3348 3620/3630 DULCYLENE ASSUNÇÃO.

8.5. Todos os custos decorrentes desta visita aos endereços do ambiente tecnológico do BANPARÁ, estão a cargo da empresa licitante, sem que caibam quaisquer indenizações, ressarcimentos ou compensações ao licitante.

9. DA SESSÃO PÚBLICA

9.1. A partir das **11h (horário de Brasília) do dia 11/02/2016** e de conformidade com o estabelecido neste Edital, terá início à sessão pública do presente Pregão Eletrônico, com a divulgação das propostas de preços recebidas em conformidade com o item 1.4 e 1.5, que deverão estar em perfeita consonância com o objeto deste edital no presente Edital e seus Anexos.

9.2. A partir desta mesma data e horário ocorrerá o início da etapa de lances, via Internet, única e exclusivamente, no *site* www.comprasnet.gov.br, conforme Edital.

10. DA FORMULAÇÃO DE LANCES

10.1. Somente os LICITANTES que apresentaram proposta de preços em consonância com o item 1.4 e 1.5, poderão apresentar lances, exclusivamente por meio do sistema eletrônico, sendo o licitante imediatamente informado do seu recebimento e respectivo horário de registro e valor.

10.2. Assim como as propostas de preços, os lances serão ofertados pelo **VALOR GLOBAL DA PROPOSTA, apurado conforme modelo do anexo II deste edital.**

10.3. Os LICITANTES poderão oferecer lances menores e sucessivos, observado o horário fixado e as regras de sua aceitação.

10.4. O LICITANTE SOMENTE PODERÁ OFERECER LANCES INFERIORES AO ÚLTIMO POR ELE OFERTADO E REGISTRADO NO SISTEMA.

10.4.1. O LICITANTE poderá ofertar outro lance menor que o seu último, independente do menor lance ofertado pelos outros licitantes concorrentes.

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

10.6. Durante o transcurso da sessão pública, os licitantes serão informados, em tempo real, do valor do menor lance registrado que tenha sido apresentado pelas demais licitantes, vedada a identificação do detentor do lance.

10.7. No caso de desconexão com a Pregoeira, no decorrer da etapa de lances, se o sistema eletrônico permanecer acessível aos licitantes, os lances continuam sendo recebidos, para a sua atuação no certame, sem prejuízo dos atos realizados.

10.8. A Pregoeira, quando possível, dará continuidade a sua atuação no certame, sem prejuízo dos atos realizados.

10.9. Quando a desconexão persistir por tempo superior a **10 (dez) minutos**, a sessão do Pregão Eletrônico será suspensa e terá reinício somente após comunicação expressa aos participantes, no endereço eletrônico utilizado para divulgação no site www.comprasnet.gov.br.

10.10. A etapa de lances da sessão pública será encerrada mediante aviso de fechamento iminente dos lances, emitido pelo próprio Sistema Eletrônico, de acordo com a comunicação às Licitantes, após o que transcorrerá período de tempo de até 30 (trinta) minutos, aleatoriamente determinado também pelo Sistema Eletrônico, findo o qual será automaticamente encerrada a recepção de lances.

10.11. Caso o Sistema não emita o aviso de fechamento iminente, a Pregoeira se responsabilizará pelo aviso de encerramento aos licitantes, observados o mesmo tempo de até 30 (trinta) minutos.

10.12. Incumbirá, ainda, ao licitante acompanhar as operações no sistema eletrônico durante o processo licitatório, responsabilizando-se pelo ônus decorrente da perda de negócios diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão. (inciso IV do art. 13 do Decreto Federal n.º 5.450/05 e inc. IV do art. 14 do Decreto Estadual n.º 2.069/2006;).

10.13. A desistência em apresentar lance implicará exclusão do licitante da etapa de lances e na manutenção do último preço por ela apresentado, para efeito de ordenação das propostas de preços.

11. DO ENCERRAMENTO DA ETAPA DOS LANCES VIA MEIO ELETRÔNICO

11.1. Encerrada a etapa de lances, a Pregoeira examinará a proposta de preços classificada em primeiro lugar quanto à compatibilidade do preço em relação ao estimado para contratação.

11.2. Caso não ocorram lances deverá ser verificado o valor estimado dos serviços e a especificação técnica prevista.

11.3. Serão rejeitadas as propostas de preços que, mesmo após os lances e negociação, ainda permaneçam superiores aos preços estimados pela Administração, tanto o preço global como os preços unitários para cada serviço que compõe o valor global.

11.4. Verificado e confirmado ser o licitante titular do menor lance empresa de médio ou grande porte, e existir microempresa(s) ou empresa(s) de pequeno porte que tenha(m) sido classificada(s) com valor de lance até 5% (cinco por cento) acima do menor lance, será aberta a oportunidade para que a microempresa ou empresa de pequeno porte melhor classificada formule lance melhor e, no caso de recusa ou impossibilidade, proceder-se-á de igual forma com as demais microempresas ou empresas de pequeno porte classificadas sucessivamente (art. 45, da Lei Complementar n° 123/2006).

11.5. Em caso de ocorrência de participação de licitante que detenha a condição de microempresa ou de empresa de pequeno porte, nos termos da Lei n.º 9.317/96 e a sua sucessora Lei Complementar n.º 123, de 14 de dezembro de 2006, serão adotados os seguintes procedimentos:

11.5.1. Será assegurada, como critério de desempate, preferência de contratação para as microempresas e empresas de pequeno porte, entendendo-se por empate aquelas situações em que as propostas apresentadas pelas microempresas e empresas de pequeno porte sejam iguais ou até 5% (cinco por cento) superiores à proposta mais bem classificada;

11.5.2. Para efeito do disposto no subitem acima, ocorrendo o empate, proceder-se-á da seguinte forma:

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

II - Não ocorrendo a contratação da microempresa ou empresa de pequeno porte, na forma do inciso anterior, serão convocadas as remanescentes que porventura se enquadrem na hipótese do subitem 11.5.2, na ordem classificatória, para o exercício do mesmo direito;

III - No caso de equivalência dos valores apresentados pelas microempresas e empresas de pequeno porte que se encontrem enquadradas no subitem 11.5.2, será realizado sorteio entre elas para que se identifique aquela que primeiro poderá apresentar melhor oferta.

11.5.3 A microempresa e a empresa de pequeno porte mais bem classificada será convocada para apresentar nova proposta no prazo máximo de 05 (cinco) minutos após o encerramento dos lances, sob pena de preclusão.

11.5.4 Na hipótese da não contratação nos termos previstos no subitem 11.5.3, o objeto licitado será adjudicado em favor da proposta originalmente vencedora do certame;

11.5.5. O disposto neste item somente se aplicará quando a melhor oferta inicial não tiver sido apresentada por microempresa ou empresa de pequeno porte.

11.6. Constatado o atendimento das exigências fixadas no Edital, a licitante será declarada vencedora.

11.7. Cumpridas as etapas anteriores, a Pregoeira verificará a habilitação do licitante conforme disposições contidas no presente Edital.

11.8. Se a proposta de preços não for aceitável ou se o licitante não atender às exigências habilitatórias, a Pregoeira examinará a proposta de preços subsequente e, assim sucessivamente, na ordem de classificação, até a apuração de uma proposta de preços que atenda ao edital, sendo o respectivo licitante declarado vencedor e a ele adjudicado o objeto do certame.

11.8.1. Ocorrendo a situação a que se refere o inciso anterior, a pregoeira poderá negociar com o licitante para que seja obtido preço melhor.

11.9. Será aceito apenas o registro de uma única proposta de preços vencedora para o LOTE, existindo a possibilidade de convocar licitantes na ordem de classificação, e assim sucessivamente, caso haja desistência da vencedora.

11.9.1. O licitante que desistir dos lances ofertados sujeitar-se-á às penalidades estabelecidas neste edital.

11.10. Atendidas as especificações do edital, estando habilitada a licitante e tendo sido aceito o menor preço apurado, a Pregoeira declarará a empresa vencedora.

11.11. A indicação do lance vencedor, a classificação dos lances apresentados e demais informações relativas à sessão pública do Pregão Eletrônico constarão de ata divulgada no sistema eletrônico, sem prejuízo das demais formas de publicidade prevista na legislação pertinente.

11.12. A proposta de preços original devidamente atualizada com o último lance deverá ser enviada, **VIA SEDEX,** ou entregue em mãos na CPL, para o BANCO DO ESTADO DO PARÁ S/A, no endereço Av. Presidente Vargas, 251 – 1º andar – Belém-Pará – Bairro do Comércio - Belém – PA, CEP: 66.010-000 no prazo máximo de 02 (dois) dias úteis da indicação do(s) licitante(s) vencedora(s).

12. DOS CRITÉRIOS DE JULGAMENTO DA PROPOSTA DE PREÇOS

12.1. O julgamento da Proposta de preços dar-se-á pelo critério de **MENOR PREÇO GLOBAL**, observadas as especificações técnicas e os parâmetros mínimos de desempenho definidos no Edital.

12.1.1. Serão rejeitadas as propostas de preços que estejam superiores aos preços estimados pela Administração, tanto o preço global como os preços unitários para cada serviço que compõe o valor global.

12.2. A Pregoeira efetuará o julgamento das Propostas de Preços, e poderá negociar pelo sistema eletrônico, diretamente com o licitante que tenha apresentado o lance de menor valor, bem assim decidir sobre sua aceitação.

12.3. O empate entre dois ou mais licitantes somente ocorrerá quando houver igualdade de preços entre a proposta de preços e quando não houver lances para definir o desempate, considerando-se, também, os procedimentos legais previstos para microempresa ou de empresa de pequeno porte.

Neste caso o desempate ocorrerá por meio de sorteio a ser realizado em sessão pública a ser designada para a qual todos os licitantes serão convocados.

12.4. Será admitido apenas 01(um) licitante vencedor.

12.5. Não será motivo de desclassificação as simples omissões que sejam irrelevantes para o entendimento da proposta de preços, que não venham causar prejuízo para o BANPARÁ S/A e nem firam os direitos dos demais licitantes.

12.6. O resultado desta licitação será publicado no Diário Oficial do Estado do Pará e no site **www.comprasnet.gov.br**.

13. DA HABILITAÇÃO

13.1. Para habilitação neste Pregão Eletrônico, a empresa interessada deverá estar cadastrada no Sistema de Cadastramento Unificado de Fornecedores - SICAF, com os documentos em plena validade, a qual será verificada "on line", atendendo, ainda, às seguintes condições:

13.1.1. Apresentar **DECLARAÇÃO DE INEXISTÊNCIA DE FATO SUPERVENIENTE IMPEDITIVO DE SUA HABILITAÇÃO**, atestando a inexistência de circunstâncias que impeçam a empresa de participar do processo licitatório, nos termos do modelo constante do **Anexo VII** deste Edital, assinada por sócio, dirigente, proprietário ou procurador da Licitante, com o número da identidade do declarante.

13.1.2. DECLARAÇÃO DO LICITANTE 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 termos do inciso XXXIII, do art. 7º, da Constituição Federal de 1988, conforme modelo constante do **Anexo VIII** deste Edital;

13.1.3. Apresentar a seguinte documentação técnica:

a) Atestado(s)/certidão(ões) de capacidade técnica fornecido(a)(s) por pessoas jurídicas de direito público ou privado, devidamente registrado na entidade profissional competente, que comprove(m) que o proponente prestou/presta serviços de natureza similar de mesma complexidade ao solicitado, inclusive com características compatíveis para fins de comprovação do item 3.3.1 do Termo de Referência.

b) Declaração de atendimento da LICITANTE aos requisitos de Infraestrutura dos centros de operações de segurança (SOC) especificados no item 3.1 do Termo de Referência, disponibilizando o ambiente para auditoria por parte do BANPARÁ;

c) Certificados em nome dos profissionais para fins de comprovação do item 3.2.5 do Termo de Referência, bem como, cópias dos documentos exigidos no item 3.2.6 do Termo de Referência referente ao vínculo destes profissionais;

d) Declaração dos fabricantes das soluções, para fins de comprovação do item 3.3.2 deste Termo de Referência;

e) Atestado de Visita Técnica, para fins de comprovação do item 9 (VISITA TÉCNICA) do termo de referência.

13.1.4. Habilitação jurídica:

a) Registro comercial, no caso de empresa individual;

b) Ato constitutivo, estatuto ou contrato social em vigor e com todas as suas alterações, ou a consolidação, se houver, devidamente registrado, em se tratando de sociedades empresárias. No caso de sociedades empresárias 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;

c) Inscrição do ato constitutivo no órgão competente acompanhada, no caso de sociedades civis, de prova da diretoria em exercício;

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

13.1.5. Regularidade fiscal:

a) Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas – CNPJ;

b) Prova de regularidade com as fazendas públicas: federal (inclusive dívida ativa), 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 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).”

c) Prova de Regularidade com o Instituto Nacional do Seguro Social – INSS;

d) Prova de Regularidade com Fundo de Garantia por Tempo de Serviço - FGTS.

e) Certidão Negativa de Débitos Trabalhistas – CNDT

f) Declaração contendo o número da inscrição Estadual e/ou Municipal, conforme o caso. Caso umas das inscrições ou ambas não se apliquem no caso concreto, a empresa deverá declarar.

13.1.6. Qualificação econômico-financeira:

a) Balanço Patrimonial e demonstrações contábeis do último exercício social, já exigíveis e apresentados na forma da lei, vedada a substituição por balancetes ou balanços provisórios, podendo ser atualizados por índices oficiais, quando encerrados há mais de 03 (três) meses da data da Sessão Pública. Devem ser nomeados os valores do Ativo Circulante (AC) e do Passivo Circulante (PC), de modo a extrair-se Índice de Liquidez Geral (LG), Índice de Liquidez Corrente (LC) e Solvência Geral**, superior a um (>1)**, resultante da aplicação da seguinte fórmula, com os valores extraídos de seu Balanço Patrimonial ou apurados mediante consulta *on line* no caso de empresas inscritas no SICAF:

$$\mathbf{LG} = \frac{\text{Ativo Circulante + Realizável a Longo Prazo}}{\text{Passivo Circulante + Exigível a Longo Prazo}}$$

$$\mathbf{LC} = \frac{\text{Ativo Circulante}}{\text{Passivo Circulante}}$$

$$\mathbf{SG} = \frac{\text{Ativo Total}}{\text{Passivo Circulante + Exigível a Longo Prazo}}$$

a.1) A licitante que apresentar índices econômicos **iguais ou inferiores a um (≤1)** em qualquer dos índices de Liquidez Geral, Solvência Geral e Liquidez Corrente, deverá comprovar que possui capital social mínimo ou patrimônio líquido mínimo de 10% (dez por cento) do valor da contratação.

b) As empresas que, porventura, ainda não tiverem concluído seu primeiro exercício social e, consequentemente, não possuírem Balanço Patrimonial exigível na forma da lei, poderão participar da licitação mediante apresentação do Balanço de Abertura, em conformidade com a legislação contábil, para a comprovação de sua qualificação econômico-financeira.

c) Certidão negativa de falência ou recuperação judicial ou Extrajudicial, expedida pelo Cartório Distribuidor da sede da pessoa jurídica; **sendo que as Certidões que não expressem a validade, só serão admitidas como válidas se emitidas a menos de 180 (cento e oitenta) dias anteriores à abertura da sessão.**

13.2. O licitante que for declarado vencedor do presente Pregão, **deverá inserir como anexo, no sistema comprasnet, todos os documentos necessários para habilitação**, a proposta de preços atualizada com o último lance (ver modelo do **Anexo II**), no prazo a ser fixado pela Pregoeira no momento da sessão pública, sendo que o referido prazo não poderá ser inferior a 60 (sessenta) minutos, prorrogáveis a critério da Pregoeira.

13.2.1. Os documentos necessários à habilitação quando estiverem desatualizados no Sistema SICAF ou quando não estiverem nele contemplados, também deverão ser inseridos, como anexo, no sistema comprasnet, conforme os prazos estabelecidos no item 13.2.

13.2.2 – Para fins de selecionar a proposta mais vantajosa para a Administração, no decorrer da análise dos documentos de habilitação e proposta de preços pela Pregoeira, este poderá diligenciar os referidos documentos e propostas, bem como, solicitar que sejam inseridos, como anexo, documentos atualizados até o prazo final agendado para o retorno da sessão.

13.2.3. Quando a proposta de preços e as declarações constantes dos itens 13.2.1 e 13.2.2 forem assinadas por um preposto da empresa que não seja seu sócio administrador ou proprietário, o licitante também **deverá inserir, como anexo, instrumento público ou particular de procuração ou documento equivalente, com firma reconhecida, com poderes especiais para responder, formular ofertas e lances de preços, recorrer e praticar todos os demais atos pertinentes ao certame, em nome do proponente.**

13.2.4. O licitante que deixar de inserir, como anexo, no sistema comprasnet, a documentação acima especificada no prazo definido pela Pregoeira será DESCLASSIFICADO do certame.

13.3. O licitante que for declarado vencedor do presente Pregão Eletrônico deverá enviar os originais e/ou autenticados dos documentos e propostas que foram inseridos, como anexo, no sistema comprasnet, na forma do item 12.3, para o BANPARÁ S/A, no prazo máximo de 02 (dois) dias úteis VIA SEDEX ou entregar na CPL, situada na Av. Presidente Vargas, 251 1º andar – Comércio – Belém –Pará – CEP- 66.010.000, em dias úteis, no horário de 09h às 16h.

13.4. As microempresas e empresas de pequeno porte, por ocasião da participação em certames licitatórios, **deverão apresentar toda a documentação exigida para efeito de comprovação de regularidade fiscal, mesmo que esta apresente alguma restrição;**

13.4.1 Havendo alguma restrição na comprovação da regularidade fiscal, será assegurado o **prazo de 05 (CINCO) dias úteis**, cujo termo inicial corresponderá ao momento em que o proponente for declarado o vencedor do certame, prorrogáveis por igual período, a critério

da Administração Pública, para a regularização da documentação, pagamento ou parcelamento do débito, e emissão de eventuais certidões negativas ou positivas com efeito de certidão negativa;

13.4.2. A não regularização da documentação, no prazo previsto no subitem anterior, implicará decadência do direito à contratação, sem prejuízo das sanções previstas no art. 81 da Lei no 8.666, de 21 de junho de 1993, sendo facultado à Administração convocar os licitantes remanescentes, na ordem de classificação, ou revogar a licitação.

13.5. Não serão aceitos "protocolos de entrega" ou "solicitação de documento" em substituição aos documentos requeridos no presente Edital e seus Anexos.

13.6. A licitante estrangeira deverá apresentar todos os documentos equivalentes aos exigidos as Licitantes brasileiras, autenticados pelos respectivos consulados ou embaixadas e traduzidos por tradutor juramentado no Brasil, no caso de ser considerada vencedora.

13.7. O não atendimento de qualquer das condições aqui previstas provocará a inabilitação do licitante.

14. DOS RECURSOS

14.1. Qualquer licitante poderá, durante a sessão pública, de forma imediata e motivada, explicitando sucintamente suas razões, imediatamente após a divulgação da vencedora, exclusivamente em campo próprio do Sistema Eletrônico, manifestar sua intenção de recorrer.

14.2. Será concedido ao licitante que manifestar a intenção de interpor recurso o prazo de 03 (três) dias úteis para apresentar as razões de recurso, ficando os demais licitantes, desde logo, intimados para, querendo, apresentarem contrarrazões em igual prazo, que começará a contar do término do prazo do recorrente, sendo-lhes assegurada vista imediata dos elementos indispensáveis a defesa dos seus interesses.

14.3. A falta de manifestação imediata e motivada do licitante importará a decadência do direito de recurso e adjudicação do objeto pela Pregoeira ao vencedor.

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

14.5. No julgamento da habilitação e das propostas, a Pregoeira poderá sanar erros ou falhas que não alterem a substância das propostas, dos documentos e sua validade jurídica, mediante despacho fundamentado, registrado em ata e acessível a todos, atribuindo-lhes validade e eficácia para fins de habilitação e classificação.

14.6. Decididos os recursos e constatada a regularidade dos atos praticados, a Autoridade Competente adjudicará o objeto e homologará o resultado da licitação para determinar a contratação.

14.7. Os autos do processo permanecerão com vista franqueada aos interessados, no BANCO DO ESTADO DO PARÁ S/A, localizado à Av. Presidente Vargas, 251 – 6º andar – Bairro do Comércio – Belém-Pará– CEP: 66.010-000, no horário de 9h às 16h (horário local).

14.8. Apenas serão considerados e analisados as razões de recursos e contra-recursos interpostos tempestivos e exclusivamente, em campo próprio do Sistema Eletrônico do comprasnet, salvo os anexos, quando necessário, poderão ser encaminhados via email cpl@banparanet.com.br ou fax (91) 3348-3303 ou (91) 3348-3216.

15. DA ADJUDICAÇÃO E DA HOMOLOGAÇÃO

15.1. A adjudicação e homologação somente serão efetivadas:

a) Se não houver manifestação das licitantes da intenção de interpor recursos, devidamente registrada em ata durante o transcurso da sessão do Pregão;

b) Após o deferimento ou indeferimento dos recursos interpostos e dado conhecimento dos seus resultados.

15.2. A adjudicação do objeto ao licitante vencedor será **GLOBAL** e ficará sujeita à homologação da autoridade competente.

15.3. Se, por motivo de força maior, a adjudicação não puder ocorrer dentro do período de validade da proposta, e, em havendo interesse do BANPARÁ, este poderá solicitar prorrogação geral da validade acima referida, por igual prazo, no mínimo.

15.4. EM OBSERVÂNCIA AO DISPOSTO NO ITEM 20.1 ABAIXO, A EMPRESA VENCEDORA DEVERÁ APRESENTAR O NÚMERO DA AGÊNCIA E CONTA CORRENTE ABERTA NO BANPARÁ, CUJA ABERTURA, OBRIGATORIAMENTE, DEVERÁ SER FEITA NO PRAZO MÁXIMO DE ATÉ 05 (CINCO DIAS) CONSECUTIVOS CONTADOS DA ASSINATURA DO CONTRATO.

16. DO PRAZO PARA ASSINATURA DO CONTRATO

16.1. Depois de homologado o resultado desta licitação, o BANPARÁ convocará a licitante adjudicatária para a assinatura do Contrato (Anexo X).

16.2. A convocação de que trata o subitem anterior deverá ser atendida no prazo máximo de 05 (cinco) dias úteis, prorrogável uma única vez, a critério do BANPARÁ, sob pena de decair o direito à contratação, sem prejuízo das sanções previstas em lei.

16.3. É facultado ao BANPARÁ, quando o proponente vencedor se recusar a assinar o contrato no prazo e nas condições estabelecidas ou não apresentar situação regular no ato de assinatura do contrato, rescindir o contrato por inadimplência, convocar os licitantes remanescentes, na ordem de classificação, para fazê-lo em igual prazo, ou revogar a licitação, independentemente das sanções previstas neste Edital.

16.4. A recusa injustificada do licitante vencedor de assinar o contrato dentro do prazo estabelecido pelo BANPARÁ caracteriza o descumprimento total das obrigações assumidas, sujeitando-a as penalidades legalmente estabelecidas.

17. DAS OBRIGAÇÕES DA LICITANTE ADJUDICATÁRIO/CONTRATADO

17.1. Além das obrigações expostas em Termo de Referência (Anexo I), o ADJUDICATÁRIO/CONTRATADO fica vinculado a:

a) Dar integral cumprimento ao objeto desta licitação, à legislação vigente, a todas as normas vigentes, à sua proposta, bem como às necessidades e orientações do BANPARÁ;

b) Assinar o contrato, relativa ao objeto que lhe for adjudicado;

c) Cumprir fielmente as obrigações enunciadas na Minuta do Contrato – Anexo XVI deste edital;

d) Prestar GARANTIA na forma do art. 56 da lei nº 8.666/93**;**

e) Prestar os serviços nos prazos estabelecidos pelo Banpará, bem como em conformidade com as especificações e condições exigidas no **Termo de Referência** (Anexo I) e demais anexos do edital . Caso a entrega não seja feita dentro do prazo ou fora das especificações exigidas no edital, o **CONTRATADO** ficará sujeito às penalidades estabelecidas neste edital e na lei n.º 8.666/93;

f) Fornecer os equipamentos e serviços de primeira qualidade, conforme as orientações contidas neste Termo de Referência e demais anexos do edital;

g) Responder pelos encargos fiscais e comerciais resultantes da adjudicação deste Pregão;

h) Responder, integralmente, por perdas e danos que vier a causar ao BANPARÁ ou a terceiros em razão de ação ou omissão, dolosa ou culposa, sua ou dos seus prepostos, independentemente de outras cominações contratuais ou legais a que estiver sujeita;

i) Abrir conta-corrente no BANPARÁ, na forma do que dispõe o Decreto Estadual n° 877/2008.

j) Manter-se durante a execução dos serviços em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas por lei e neste edital, bem como, quanto ao cumprimento da emenda constitucional nº 42 à Constituição do Estado do Pará, de 04 de junho de 2008, devendo a empresa contratada, por ocasião da retirada da nota de empenho, apresentar declaração de que emprega pessoas com deficiência, na forma prevista na referida emenda;

k) Emitir Nota Fiscal Eletrônica – Nfe, modelo 55, nos termos do Protocolo ICMS 42/2009 de 03 de julho de 2009, se for o caso.

17.2. O ADJUDICATÁRIO/CONTRATADO não será responsável:

a) Por qualquer perda ou dano resultante de caso fortuito ou força maior;

b) Por quaisquer trabalhos, serviços ou responsabilidades não previstos neste Edital.

17.3. O BANPARÁ não aceitará, sob nenhum pretexto, a transferência de responsabilidade do ADJUDICATÁRIO/CONTRATADO para outras entidades, sejam fabricantes, representantes ou quaisquer outros.

17.4. O contratado deverá prestar garantia ao BANPARÁ, conforme previsto no art. 56 da Lei 8.666/93, no prazo e nas condições estabelecidas na **Minuta de Contrato** (Anexo XVI).

18. DAS OBRIGAÇÕES DO BANPARÁ

18.1. Além das obrigações expostas em Termo de Referência (Anexo I) O BANPARÁ, após a assinatura do contrato, compromete-se a:

a) Proporcionar todas as facilidades indispensáveis à boa execução das obrigações contratuais, inclusive permitindo o acesso de empregados, prepostos ou representantes do CONTRATADO, se for o caso, desde que estejam devidamente identificados, aos locais onde os objetos serão entregues, em horário adequado e no tempo necessário para sua entrega;

b) Prestar todas as informações, todos os dados necessários para a execução do objeto contratado, observados o sigilo profissional e o bancário;

c) Promover os pagamentos na forma convencionada e dentro do prazo estipulado para tal;

d) Atestar as faturas correspondentes aos objetos entregues;

e) Comunicar ao CONTRATADO toda e qualquer ocorrência relacionada com a entrega dos equipamentos;

f) Acompanhar e fiscalizar a entrega dos objetos, por meio de funcionário indicado e designado como representante do BANPARÁ.

19. DAS CONDIÇOES DE ENTREGA E IMPLANTAÇÃO DOS SERVIÇOS

19.1. Os serviços serão prestados na forma e nos prazos previstos no **Item 12 e demais subitens do termo de referência**, anexo I do edital, bem como, nos demais anexos e na minuta do contrato.

19.2. Os serviços prestados em desacordo com o especificado neste instrumento convocatório e na proposta da ADJUDICATÁRIA serão considerados inexecução total do contrato, sujeito às penalidades nele prevista.

20. DA FISCALIZAÇÃO DA EXECUÇÃO CONTRATUAL

20.1. O fornecimento dos bens objeto deste Pregão será fiscalizado, conforme o caso, por um empregado ou por uma Comissão composta de no mínimo 3 (três) empregados do BANPARÁ, doravante denominada FISCALIZAÇÃO, com autoridade para exercer, como representante da Administração do BANPARÁ, toda e qualquer ação de orientação geral, acompanhamento e fiscalização da execução contratual.

21. DO PAGAMENTO

21.1. O pagamento será efetuado, nos termos do **item 14** e seus subitens do Termo de Referência, Anexo I deste edital e **exclusivamente** por crédito em conta-corrente da ADJUDICATÁRIA/CONTRATADA aberta no BANPARÁ, conforme art. 2º do Decreto Estadual n.º 877/2008 de 31/03/2008, quando mantidas as mesmas condições iniciais de habilitação neste certame e observadas as seguintes condições:

a) Será efetuada a retenção na fonte dos tributos e contribuições exigidos pela legislação em vigor, tais como, IR, ICMS, CSLL, COFINS, PIS/PASEP, etc.

b) Apresentação do número da agência e conta corrente aberta no Banpará, cuja abertura, obrigatoriamente deverá ser feita no prazo MÁXIMO DE ATÉ 05 (CINCO DIAS) CONSECUTIVOS CONTADOS DA ASSINATURA DO CONTRATO.

c) A Contratada, optante pelo Simples, deverá apresentar, juntamente com a nota fiscal/fatura, declaração, conforme modelo constante do Anexo IV da Instrução Normativa SRF nº 480, de 15/12/2004, substituído pelo Anexo IV constante da IN RFB n° 791, de 10 de dezembro de 2007. Caso não o faça, ficará sujeita à retenção de imposto e contribuições, de acordo com a referida Instrução.

d) As Notas Fiscais/Faturas e Documentações entregues em desacordo serão devolvidas pelo **BANPARA** com as informações que motivaram a rejeição, contando novo prazo para o efetivo pagamento, após visto e homologação na Fatura, exarados pela área técnica. A devolução de notas/faturas não servirá de pretexto para a suspensão dos serviços ou ao descumprimento de cláusulas contratuais.

e) Caso verificada a situação de descumprimento das condições de habilitação, nos termos do art. 55, inc XIII da Lei 8.666/93, será o CONTRATADO notificado para, em até 15 dias, regularizar a situação, sob pena de instauração de procedimento administrativo, com garantia de ampla defesa e contraditório, com finalidade de aplicação das penalidades previstas na Cláusula dez deste Contrato.

21.2. A contratada se obrigará a utilizar a Nota Fiscal Eletrônica NF-e Modelo 55, em substituição a Nota Fiscal Modelo 1 ou 1-A (modelo antigo), na totalidade das operações de compras efetuadas pelas Unidades do CONTRATANTE, independente da atividade econômica exercida. Assim sendo, nenhuma nota fiscal modelo 1 ou 1-A será aceita, mesmo que dentro do prazo de validade de uso. Os demais modelos de notas fiscais e cupom fiscal continuam em vigor.

21.3 Ocorrendo atraso no pagamento das faturas ou outros documentos de cobrança emitidos pela **CONTRATADA,** desde que não haja culpa da **CONTRATADA**, incidirá sobre os valores em atraso juros de mora no percentual de 1% (um por cento) ao mês, *pro rata die*, calculados de forma simples sobre o valor em atraso e devidos a partir do dia seguinte ao do vencimento até a data da efetiva liquidação do débito.

21.4. Os valores contratados serão reajustados anualmente, a contar da data da apresentação formal pela ADJUDICATÁRIA/CONTRATADA de sua proposta de preços, segundo a variação acumulada do INPC do Instituto Brasileiro de Geografia e Estatística – IBGE, ou outro, na falta deste, que estiver estabelecido na legislação à época de cada reajuste.

22. DAS PENALIDADES

22.1. O **LICITANTE** será sancionado com o impedimento de licitar e contratar com o BANPARA e será descredenciado no SICAF e no cadastro de fornecedores do BANPARA, pelo prazo de até 5 (cinco) anos, e demais cominações legais, nos seguintes casos:

a) Cometer fraude fiscal;

b) Apresentar documento falso;

c) Fizer declaração falsa;

d) Comportar-se de modo inidôneo. Reputar-se-ão inidôneos atos como os descritos nos art.s 90, 92, 93, 94, 95 e 97 da Lei nº 8.666/93;

e) Não assinar o contrato ou retirar a nota de empenho no prazo estabelecido;

f) Deixar de entregar a documentação exigida no certame;

g) Não mantiver a proposta, incidindo também nesta hipótese a não apresentação dos documentos exigidos na licitação.

22.2. Na análise do descumprimento, quanto aos itens "f" e "g", desde que o ato da licitante não resulte em prejuízos para o BANPARA, poderá ser aplicada a penalidade de ADVERTÊNCIA.

22.3. Verificado o descumprimento ao presente Edital, a Pregoeira, solicitará mediante e-mail a apresentação de defesa no prazo de 05 (cinco) dias.

22.3.1. Findo o referido prazo, com apresentação ou não das razões da empresa, a Pregoeira, submeterá o processo à Diretoria Administrativa, com sugestão quanto ao arquivamento ou aplicação de penalidade, para decisão;

22.3.2. Da decisão o LICITANTE será notificado mediante e-mail ou carta com Aviso de Recebimento, para querendo, apresentar eventual recurso à decisão no prazo de 05 (cinco) dias, o qual será julgado pela Presidência da Instituição.

22.4. A não apresentação de documentos comprobatórios de situação regular, em especial no que se refere ao INSS e ao FGTS, necessariamente apresentados em atendimento às exigências de habilitação (art. 55, XIII, Lei 8.666/93), pode gerar a aplicação das penalidades previstas no art. 87 da mesma lei, assim como rescisão contratual, nos termos do art. 77 e seguintes, da mesma legislação acima mencionada.

23. DAS CONDIÇÕES DE CONTRATAÇÃO

23.1. A empresa **CONTRATADA,** como condição prévia da assinatura do Instrumento Contratual, deverá apresentar Declaração de que emprega pessoas com deficiência, na forma prevista na Emenda Constitucional nº 42, de 04 de junho de 2008, à Constituição do Estado do Pará.

24. DAS ALTERAÇÕES:

24.1. Eventuais alterações contratuais reger-se-ão pela disciplina do art. 65 da Lei nº 8.666, de 1993.

24.2. A CONTRATADA é obrigada a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessário, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado adjudicado.

25. DA FRAUDE E DA CORRUPÇÃO

25.1. Os licitantes deverão observar os mais altos padrões éticos durante o processo licitatório, estando sujeitos às sanções previstas na legislação brasileira.

26. DO FORO

26.1. As questões decorrentes da execução deste edital, que não possam ser dirimidas administrativamente, serão processadas e julgadas na Justiça Comum, no Foro da cidade de Belém/PA, com exclusão de qualquer outro, por mais privilegiado que seja.

27. DAS DISPOSIÇÕES FINAIS

27.1. Esta licitação poderá ser revogada total ou parcialmente, ou ainda anulada, sem que caiba indenização aos licitantes em consequência do ato, nos termos da legislação vigente.

27.2. A presente licitação poderá ter a sua abertura adiada ou transferida para outra data, mediante aviso prévio.

27.3. Os documentos exigidos neste procedimento licitatório poderão ser apresentados em original, por meio de fotocópias autenticadas por cartório competente ou servidor da administração, ou fotocópias simples (exceto cópia de FAX) acompanhadas dos originais para cotejo no ato da apresentação.

27.4. As normas que disciplinam este pregão eletrônico serão sempre interpretadas em favor da ampliação da disputa entre os interessados, sem comprometimento da segurança da futura contratação.

27.5. Os licitantes assumem todos os custos de preparação e apresentação de suas propostas e o BANPARÁ não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do processo licitatório.

27.6. Nenhuma indenização ou ressarcimento serão devidos aos licitantes pela elaboração de proposta ou apresentação de documentos ou ainda, quando for o caso, apresentação de amostras relativa a esta licitação.

27.7. Da sessão será lavrada ata eletrônica com a relação das licitantes e todas as ocorrências que interessarem ao certame.

27.8. Sem prejuízo das disposições contidas no Capítulo III – Dos Contratos da Lei n.º 8.666/93, o presente Edital e a proposta do ADJUDICATÁRIO serão partes integrantes do contrato a ser firmada com o ADJUDICATÁRIO.

27.9. O instrumento de contrato a ser assinado com a adjudicatária poderá ser alterado nos casos previstos no art. 65 da Lei n.º 8.666/93, desde que haja interesse da Administração Pública.

27.10. A Pregoeira ou autoridade superior poderão promover diligências destinadas a elucidar ou complementar a instrução do processo, em qualquer fase da licitação.

27.11. Os licitantes são responsáveis pela fidelidade e legitimidade das informações e dos documentos apresentados em qualquer fase da licitação.

27.12. A homologação do resultado desta licitação não implicará direito à contratação do objeto pelo BANPARÁ.

27.13. Para fins de aplicação das sanções administrativas constantes no presente edital, o lance é considerado proposta de preços.

27.14. O desatendimento de exigências formais não essenciais, não importará no afastamento do licitante, desde que seja possível a aferição da sua qualificação, e a exata compreensão da sua proposta de preços, durante a realização da sessão pública do Pregão eletrônico.

27.15. A Pregoeira, ou autoridade superior, poderá subsidiar-se em pareceres emitidos por técnicos ou especialistas no assunto objeto desta licitação.

27.16. Em caso de discrepância entre os anexos e o Edital prevalecerá a redação do instrumento convocatório.

27.17. A Pregoeira não desclassificará ou inabilitará, qualquer licitante por falta de rubrica, erros ou omissões que não prejudiquem o curso do processo e possa satisfazer as exigências dentro da sessão.

2.18. Para a participação exclusiva de microempresas e empresas de pequeno porte, aplicar-se-ão, no curso desta licitação, as determinações contidas na Lei Complementar n.º 123/2006, as quais deverão comprovar sua condição quando da apresentação dos documentos relativos à habilitação.

27.19. Aplicam-se, a presente licitação, subsidiariamente, as Leis n.º 8.078/1990 - Código de Proteção e Defesa do Consumidor e demais normas legais pertinentes.

27.20. O edital e seus anexos, além de poderem ser lidos e retirados através da internet nos sites **www.comprasnet.gov.br**, **www.banpara.b.br** e **www.compraspara.pa.gov.br** poderão também ser obtidos no BANPARÁ, situado Av. Presidente Vargas, 251 –1º andar, no horário de 9 às 16h, em dias úteis.

27.21. Para consulta nos autos quando necessário ao perfeito entendimento deste edital, poderá ser contactada à Comissão Permanente de Licitações, pessoalmente, no endereço Av. Presidente Vargas, 251 – 1º andar – Sala de licitações – Belém-Pa, ou através do telefone/fax (91) 3348-3391 ou fones (91) 3348-3392 e (91) 3348-3303, entre 9h e 16h ou ainda pelo e-mail cpl@banparanet.com.br.

27.22. Toda comunicação oficial se dará através de correspondência com AR ou fac-símile ou por publicação ou ainda, por e-mail, nos termos da legislação.

Belém-Pará, 26 de Janeiro de 2016

Manuele Silva
Pregoeira

1. OBJETO. Contratação de empresa especializada no fornecimento de Solução Integrada de Serviços Gerenciados de Segurança Lógica, no modelo 24 horas por dia, 7 dias por semana, 365 dias por ano, inicialmente por 48 meses, incluindo o conjunto de hardware e software fornecidos em regime de comodato, necessários e suficientes para a prestação desses serviços, de acordo com o seguinte escopo:

- Serviço de Firewall Próxima Geração e VPN, para controle do tráfego nos segmentos protegidos;
- Serviço de Prevenção de Intrusos, para detecção e bloqueio de intrusão nos segmentos protegidos;
- Serviço de Gestão de Risco e Compliance, para descoberta e gestão de eventuais falhas de segurança no ambiente;
- Serviço de Gateway de E-mail e Web, para controle do tráfego de e-mail e proteção contra vírus, spam e conteúdo indesejado, assim como para controle do tráfego de internet e proteção contra vírus, acessos indevidos e conteúdo indesejado;
- Serviço de Proteção das Estações de Trabalho e Servidores de Rede (Tanto físicos, quanto virtuais) para identificar e mitigar infecções por vírus;
- Serviço de Proteção Contra Vazamento e Integridade dos Dados, para identificar e mitigar possíveis perdas de informações sensíveis;
- Serviço de Gestão de Eventos e Incidentes, para armazenagem, gerenciamento e correlacionamento de logs e eventos;
- Serviço de Proteção Contra Ameaças Dia Zero, para identificar e bloquear esse tipo de ameaça no ambiente da CONTRATANTE;
- Serviço de Monitoramento e Proteção de Base de Dados, para monitorar, identificar e controlar acesso aos bancos de dados;
- Disponibilização de banco de até 4.000 (mil) horas para a prestação de serviços técnicos, que possam ser utilizadas sob demanda.

2. DESCRIÇÃO DOS SERVIÇOS

2.1. IMPLANTAÇÃO DAS SOLUÇÕES

2.1.1. A CONTRATADA deverá oferecer implantação das soluções realizadas pela(s) FABRICANTE(S), com configuração, instalação, testes e fornecimento dos hardwares e softwares relacionados, em regime de comodato, para o seguinte escopo:

2.1.1.1. Serviço de Contra Vazamento e Integridade dos Dados;

2.1.1.2. Serviço de Gestão de Eventos e Incidentes;

2.1.1.3. Serviço de Proteção Contra Ameaças Dia Zero;

2.1.1.4. Serviço Monitoramento e Proteção de Base de Dados;

2.1.1.5. Para os serviços supracitados nos itens 2.1.1.1 a 2.1.1.4 deverão ser apresentados os seguintes entregáveis durante a implantação:

2.1.1.5.1. Fase de Desenho da arquitetura realizada pela(s) FABRICANTE(S):

2.1.1.5.1.1. Esquema detalhado de Conexão com dispositivos;
2.1.1.5.1.2. Carta Gantt de Atividades.

2.1.1.5.2. Fase de Instalação realizada pela(s) FABRICANTE(S):

2.1.1.5.2.1. Envio de resumo semanal com atividades realizadas, avanços e problemas detectados.

2.1.1.5.3. Fase de pós instalação realizada pela(s) FABRICANTE(S):

2.1.1.5.3.1. A(S) FABRICANTE(S) confeccionará(ão) relatório(s) final(is) sobre as atividades realizadas e recomendações à CONTRATANTE. Este relatório será entregue 25 dias úteis após a realização dos trabalhos. No relatório entregue constarão as seguintes seções:

2.1.1.5.3.1.1. Introdução;
2.1.1.5.3.1.2. Análise do ambiente;
2.1.1.5.3.1.3. Atividades realizadas;
2.1.1.5.3.1.4. Configuração de políticas aplicadas;
2.1.1.5.3.1.5. Resultados obtidos (Coberturas, eventos de segurança registrados);
2.1.1.5.3.1.6. Conclusões;
2.1.1.5.3.1.7. Recomendações Específicas;
2.1.1.5.3.1.8. Recomendações de Segurança Corporativa.

2.1.2. A CONTRATADA deverá oferecer implantação das soluções realizadas pela CONTRATADA baseada em arquitetura desenhada pela(s) FABRICANTE(S) e com validação final da solução realizada pela(s) FABRICANTE(S), com configuração, instalação, testes e fornecimento dos hardwares e softwares relacionados, em regime de comodato, para o seguinte escopo:

2.1.2.1. Serviço de Firewall Próxima Geração e VPN;

2.1.2.2. Serviço de Prevenção de Intrusos;

2.1.2.3. Serviço de Gestão de Risco e Compliance;

2.1.2.4. Serviço de Gateway de E-mail e Web;

2.1.2.5. Serviço de Proteção das Estações de Trabalho e Servidores de Rede;

2.1.2.6. Para os serviços supracitados nos itens 2.1.2.1 a 2.1.2.5 deverão ser apresentados os seguintes entregáveis durante a implantação:

2.1.2.6.1. Fase de Desenho da arquitetura realizada pela(s) FABRICANTE(S):

2.1.2.6.1.1. Esquema detalhado de Conexão com dispositivos;
2.1.2.6.1.2. Carta Gantt de Atividades.

2.1.2.6.2. Fase de Instalação realizada pela CONTRATADA:

2.1.2.6.2.1. Envio de resumo semanal com atividades realizadas, avanços e problemas detectados.

2.1.2.6.3. Fase de pós instalação realizada pela CONTRATADA:

2.1.2.6.3.1. Se confeccionará um relatório final sobre as atividades realizadas e recomendações à CONTRATANTE. Este relatório será entregue 21 dias úteis após a realização dos trabalhos. No relatório entregue constarão as seguintes seções:

2.1.2.6.3.1.1. Introdução;
2.1.2.6.3.1.2. Análise do ambiente;

2.1.2.6.3.1.3. Atividades realizadas;
2.1.2.6.3.1.4. Configuração de políticas aplicadas;
2.1.2.6.3.1.5. Resultados obtidos (Coberturas, eventos de segurança registrados);
2.1.2.6.3.1.6. Conclusões;
2.1.2.6.3.1.7. Recomendações Específicas;
2.1.2.6.3.1.8. Recomendações de Segurança Corporativa.

2.1.2.6.4. Fase de pós instalação realizada pela(s) FABRICANTE(S):

2.1.2.6.4.1. Se confeccionará um relatório final sobre a solução implantada e recomendações à CONTRATANTE. Este relatório será entregue 21 dias úteis após a realização dos trabalhos. No relatório entregue constarão as seguintes seções:

2.1.2.6.4.1.1. Introdução;
2.1.2.6.4.1.2. Análise do ambiente;
2.1.2.6.4.1.3. Atividades realizadas;
2.1.2.6.4.1.4. Configuração de políticas aplicadas;
2.1.2.6.4.1.5. Resultados obtidos (Coberturas, eventos de segurança registrados);
2.1.2.6.4.1.6. Conclusões;
2.1.2.6.4.1.7. Recomendações Específicas;
2.1.2.6.4.1.8. Recomendações de Segurança Corporativa.

2.1.3. Todas as atividades envolvidas serão acompanhadas e coordenadas por analistas e técnicos do BANPARÁ;

2.1.4. A implantação das soluções, quando realizadas no ambiente de produção, poderão ter as atividades executadas após o expediente (horários noturnos ou em finais de semana e feriados);

2.1.5. A CONTRATADA será responsável por efetuar as atividades de integração da solução de monitoração remota com o ambiente operacional do BANPARÁ, sem prejuízo aos serviços desta;

2.1.6. Quando previamente acordado entre as partes, a CONTRATADA poderá realizar serviços de monitoramento in loco com o acompanhamento de um representante da instituição.

2.1.7. A instalação dos equipamentos e sistemas que permitirão a prestação dos serviços de que trata este Termo de Referência deverá ser executado pela CONTRATADA nos prédios do BANPARÁ localizados respectivamente, na Rua Municipalidade Nº 1036 – Bairro: Umarizal, CEP: 66050350, e na Matriz localizado na Av. Pte. Vargas Nº 251, Bairro: Centro, CEP: 66010000, sem custos adicionais para o BANPARÁ;

2.2. PRESTAÇÃO DOS SERVIÇOS CONTÍNUOS

2.2.1. Os serviços deverão ser prestados remotamente, a partir de Centros de Operação de Segurança (SOC) próprios, localizados no Brasil, estritamente de acordo com as especificações deste documento;

2.2.2. Os serviços de monitoração remota da segurança deverão ser realizados pela CONTRATADA, na modalidade 24x7 (vinte e quatro horas por dia, sete dias na semana);

2.2.3. Para a manutenção do hardware e software ofertados, bem como para a prestação de suporte aos serviços de monitoração remota, a CONTRATADA deve possuir infraestrutura de suporte técnico, disponível em período integral, ou seja, 24x7 (vinte e quatro horas por dia, sete dias por semana), nos seguintes modelos:

2.2.3.1. Suporte técnico remoto: suporte prestado por meio de Central de Atendimento 0800 ou equivalente à ligação local, web, e-mail e fax, para:

2.2.3.1.1. Esclarecimento de dúvidas relacionadas à prestação dos serviços, políticas e regras implementadas, funcionalidade da solução e incidentes de segurança, sendo este atendimento imediato;
2.2.3.1.2. Atendimento às solicitações de alterações (inclusão e exclusão) de políticas e regras;
2.2.3.1.3. Atendimento às solicitações de log e relatórios;

2.2.3.2. Suporte técnico local: atendimento in-loco, prestados por técnicos capacitados para a solução de problemas relacionados aos equipamentos e softwares.

2.2.3.2.1. Não será obrigatória a existência de escritório local, sediado em Belém/PA, para a prestação do suporte.
2.2.3.2.2. O profissional responsável pelo atendimento deverá ser funcionário em regime CLT ou sócio da empresa contratada.

2.2.4. As versões dos softwares ofertados pela CONTRATADA sempre deverão estar com a versão mais atual disponível no mercado. A versão anterior:

2.2.4.1. Não poderá permanecer instalada mais do que 03 (três) meses, após o lançamento da última versão homologada; ou

2.2.4.2. Poderá permanecer instalada por tempo maior, desde que acordado com o BANPARÁ.

2.2.5. Para todos os serviços, a contratada deverá criar contas de usuários para que a equipe técnica do Banpará possa acompanhar e compreender as configurações adotadas. As permissões destas contas serão definidas pelo próprio BANPARÁ, mediante assinatura de Termo de responsabilidade assinado pelo gestor da área de segurança.

2.2.6. Deverão ser apresentados pela CONTRATADA, no mínimo, relatórios analíticos mensais contendo o diagnóstico dos ambientes monitorados, obtido através do cruzamento das informações coletadas pelos softwares. Tais relatórios deverão estar disponíveis para o BANPARÁ a qualquer momento, se solicitado, devendo ser disponibilizados em até 24 (vinte e quatro) horas após a solicitação;

2.2.7. Os recursos humanos envolvidos na atividade de monitoração remota da segurança deverão ser dedicados às atividades de monitoração, ou seja, os mesmos não poderão executar outras atividades na CONTRATADA;

2.2.8. Os recursos humanos envolvidos na prestação de serviço de monitoração remota da segurança deverão estar capacitados na solução envolvida. Entende-se por capacitação: certificados profissionais emitidos pelos fabricantes das soluções que serão gerenciadas;

2.2.9. A CONTRATADA deverá interagir com os analistas e técnicos do BANPARÁ para dirimir dúvidas relacionadas ao serviço prestado;

2.2.10. A CONTRATADA deverá disponibilizar 0800 para abertura e acompanhamento de chamados e dirimir dúvidas relacionadas a prestação de serviço;

2.2.11. Os chamados abertos somente poderão ser fechados após autorização de funcionário designado pelo BANPARÁ.

2.2.12. O fechamento por parte da contratada que não tenha sido previamente autorizado pelo BANPARÁ poderá ensejar aplicação de multa a CONTRATADA no valor conforme termo de contrato do valor mensal pelos serviços por ocorrência;

2.2.13. O BANPARÁ informará as pessoas autorizadas a abrir e fechar chamados junto a CONTRATADA, bem como o meio pelo qual a autorização de fechamento será formalizada;

2.3. MANUTENÇÃO DAS REGRAS E POLÍTICAS E VERSÕES DOS SOFTWARES

2.3.1. Toda e qualquer alteração na configuração da solução (aplicação de novas regras, exclusão de regras, atualização de versões, aplicações de "patches", etc.) deverão ocorrer mediante autorização do BANPARÁ;

2.3.2. O BANPARÁ, no momento da implantação da solução, indicará as pessoas que poderão autorizar as referidas alterações. A CONTRATADA implementará mecanismos que garantem a identificação destas pessoas;

2.3.3. As alterações das configurações deverão ocorrer em horários determinados pelo BANPARÁ;

2.3.4. O tempo de atendimento das solicitações de alterações das políticas e regras feitas pelo BANPARÁ não deverá ultrapassar o SLA (acordo de nível de serviço) especificado neste documento, a contar da efetivação da solicitação;

2.3.5. A CONTRATADA deverá efetuar, em laboratório próprio, os testes necessários antes de implementar qualquer alteração no ambiente de monitoração (políticas, regras, versões, etc.), evitando impactos negativos nos serviços do BANPARÁ;

2.3.6. O BANPARÁ poderá solicitar, por escrito, o acesso às senhas de configuração dos equipamentos disponibilizados pela CONTRATADA em regime de comodato. O BANPARÁ designará duas pessoas para terem acesso a(s) senha(s), que devem ser fornecidas de forma segura. O BANPARÁ deverá seguir os procedimentos documentais acordados entre as partes, caso venha a fazer uso deste acesso, e se responsabilizará pelas conseqüências que por ventura possam advir deste acesso;

2.4. CONTROLE DOS SERVIÇOS REALIZADOS PELA CONTRATADA

2.4.1. Para o controle e administração dos serviços realizados pela CONTRATADA, o BANPARÁ poderá nomear até 12 (doze) representantes autorizados a interagir com a CONTRATADA. Tais representantes serão responsáveis por:

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

2.4.3. Definir as estratégias, políticas e regras a serem implantadas, e analisar os relatórios gerados pelos softwares que compõem a solução;

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

2.4.5. Para cada solução implantada a CONTRATADA emitirá relatórios definidos pelo BANPARÁ;

2.4.6. A CONTRATADA realizará reuniões mensais, nas dependências do BANPARÁ, para dirimir dúvidas sobre o serviço contratado, análise e entendimento dos relatórios gerenciais e administrativos e revisão das configurações e procedimentos implementados;

2.4.7. O BANPARÁ poderá realizar auditoria nas instalações do Centro de Operações de Segurança (SOC), com o objetivo de verificar as instalações físicas, a segurança física e lógica do ambiente, e demais itens exigidos neste documento, desde que previamente acordada com a CONTRATADA;

2.4.8. A CONTRATADA deverá fornecer Treinamento oficial ministrado pelo(s) fabricante(s) na cidade da CONTRATANTE, visando treinar a equipe do BANPARÁ quanto às funcionalidades e os recursos de cada produto que fazem parte da solução.

2.5. TREINAMENTO

2.5.1. O treinamento deverá ser oficial do(s) fabricante(s) e ministrado para no mínimo 8 pessoas e no máximo 12 pessoas, no ambiente do Banpará, **com carga horária praticada pelos cursos oficiais**. O material do curso deverá ser em língua portuguesa, podendo ser em língua inglesa no caso de indisponibilidade.

2.5.2. As datas dos treinamentos deverão ser estabelecidas pelo CONTRATANTE em até 60 dias após a implantação de seu respectivo serviço.

2.5.3. Ao final do treinamento a contratada deverá fornecer certificado e o Banpará deverá emitir o termo de aceite do Treinamento.

2.5.4. Caso o treinamento de qualquer um dos serviços não satisfaça em termos técnicos, o termo de aceite não será emitido e a contratada deverá ministrar novamente o curso, corrigindo os problemas apontados, sem ônus ao Banpará. Neste caso a CONTRATADA deverá realizar novo curso em até 30 dias após comunicação da CONTRATANTE do não aceite do curso;

2.5.5. Não poderá ser motivo de não aceite a ausência de funcionários e/ou analistas da CONTRATANTE nas datas estabelecidas para os treinamentos;

2.5.6. Não poderá ser motivo de não aceite a falta de entendimento do conteúdo do curso, para o caso deste material ser fornecido em língua inglesa;

2.5.7. O custo referente ao treinamento deverá está incluso no valor global do contrato e discriminado nas propostas dos licitantes, conforme ANEXO VI - MODELO PROPOSTA DE PREÇOS.

2.5.8. A data e o horário do treinamento deverão ser previamente acordados com Banpará.

2.5.9. Os custos com passagens, hospedagem, deslocamento, alimentação e material didático, para a realização do treinamento, já estarão inclusos no preço ofertado.

2.6. ARMAZENAMENTO DOS LOGS DE AUDITORIA:

2.6.1. O BANPARÁ, caso julgue insuficiente as informações gravadas nos arquivos de logs, poderá solicitar alterações na configuração junto à CONTRATADA;

2.6.2. O tempo de retenção dos logs gerados deverá ser equivalente ao prazo da vigência contratual. Ao final do contrato, a CONTRATADA não deverá ficar com nenhuma cópia dos mesmos, repassando-os para o BANPARÁ em meio magnético antes da sua destruição.

2.7. OCORRÊNCIA DE INCIDENTES

2.7.1. No caso de detecção de algum incidente de segurança, a CONTRATADA pode acionar o BANPARÁ imediatamente, para que sejam tomadas as medidas corretivas e legais necessárias, de acordo com o procedimento de resposta a incidentes;

2.7.2. Serão considerados incidentes de segurança: os acessos indevidos, instalação de códigos maliciosos, indisponibilidade dos serviços (DoS), ataques por força bruta, ou qualquer outra ação que vise prejudicar a funcionalidade dos serviços do BANPARÁ;

2.7.3. A CONTRATADA deverá comunicar imediatamente ao BANPARÁ, para que possam ser tomadas ações preventivas nos casos de tentativas de: acessos indevidos, de instalação de códigos maliciosos ou de qualquer outra ação que venham pôr em risco a segurança do ambiente do BANPARÁ, mesmo que o a pessoa não obtenha sucesso na tentativa de invasão;

2.7.4. A CONTRATADA deverá disponibilizar todas as informações necessárias (origem do ataque, tipo de ataque, data e hora, logs, etc.) para que sejam apurados os incidentes de segurança reportados;

2.7.5. Dependendo do grau do incidente, a CONTRATADA poderá deslocar recurso técnico capaz de dar suporte ao problema, para compor o tempo de resposta do BANPARÁ, visando dirimir quaisquer dúvidas e dar suporte nas providências a serem tomadas.

2.8. SOLUÇÃO DE HARDWARE E SOFTWARE DA CONTRATADA

2.8.1. Os software e hardware necessários para implantação do serviço de monitoração, gerência e administração remota da segurança fazem parte dos serviços a serem prestados pela CONTRATADA durante o prazo do contrato.

2.8.2. A manutenção das licenças do hardware e software necessários, junto aos fabricantes, será de responsabilidade da CONTRATADA, devendo as mesmas estar em nome do BANPARÁ, devendo A CONTRATADA apresentar cópia autenticada das mesmas anualmente a CONTRATANTE.

2.8.3. O hardware e software ofertados deverão ser compatíveis com o ambiente operacional do BANPARÁ.

2.8.4. A CONTRATADA é responsável pela manutenção preventiva e corretiva do hardware por ela ofertado.

2.8.5. O hardware e o software devem ser fornecidos em regime de comodato.

2.9. ENCERRAMENTO DOS SERVIÇOS DE MONITORAÇÃO REMOTA DA SEGURANÇA

2.9.1. Quando do encerramento da prestação do serviço de monitoração remota da segurança, a CONTRATADA deverá retirar os componentes da solução, comunicando a retirada ao BANPARÁ, por escrito, com 60 dias de antecedência;

2.9.2. Todas as informações de customização, políticas e regras, logs de auditoria serão disponibilizadas para o BANPARÁ, em mídia magnética ou via rede, e em seguida eliminadas da base de dados da CONTRATADA.

2.9.3. Ao final do contrato a CONTRATADA deverá dar suporte durante toda a fase de transição dos serviços à uma nova CONTRATADA se for o caso.

2.9.4. Caso haja interesse da CONTRATANTE está terá a possibilidade de adquirir os equipamentos fornecidos em comodato, o que deverá ser informado até o 45º (quadragésimo quinto) mês pela CONTRATANTE, manifestado o interesse a CONTRATADA deverá emitir proposta comercial que não deverá ultrapassar o limite de **0,1 %** do valor global ao final do contrato para aquisição dos equipamentos fornecidos em comodato.

3. DAS CONDIÇÕES PARA A PRESTAÇÃO DO SERVIÇO.

3.1. Os Centros de Operações de Segurança (SOC) já devem estar em pleno funcionamento na data da abertura deste edital e devem possuir alta disponibilidade, atendendo aos seguintes requisitos:

3.1.1. Os ativos de TI empregados no monitoramento (servidores, rede, software, etc.) deverão estar hospedados em ambiente com as seguintes características mínimas:

3.1.1.1. Possuir sistemas redundantes para armazenamento de dados e alimentação de energia;

3.1.1.2. Possuir estrutura de armazenamento de dados que permita a manutenção dos registros dos eventos relacionados aos serviços contratados por, no mínimo, o prazo do CONTRATO. Após este período deverão ser disponibilizadas para o BANPARÁ, em mídia digital ou via rede, e em seguida eliminadas da base de dados da CONTRATADA;

3.1.1.3. Estar configurados de forma que a falha de nenhum dos equipamentos isoladamente interrompa o funcionamento dos sistemas;

3.1.1.4. Estar hospedado em *Datacenter* que deve atender as seguintes especificações:

3.1.1.4.1. Possuir sistemas redundantes para armazenamento de dados e alimentação de energia;

3.1.1.4.2. Possuir estrutura de armazenamento de dados que permita a manutenção dos registros dos eventos relacionados aos serviços contratados por no mínimo 180 dias. Após este período deverão ser disponibilizadas para o contratante, em mídia digital ou via rede, e em seguida eliminadas da base de dados da CONTRATADA;

3.1.1.4.3. Possuir dispositivos redundantes para fornecer energia elétrica e controle de temperatura. Cada um destes dispositivos deve ter capacidade para manter a operação isoladamente em caso de manutenção planejada ou falha.

3.1.1.4.4. Possuir caminhos de distribuição de energia elétrica e conexões de rede local redundantes de modo que um caminho permaneça ativo e o outro possa ser utilizado como alternativa em caso de manutenção planejada ou falha. Os sistemas de distribuição que devem ser considerados nessa especificação são:

3.1.1.4.4.1. Cabine para recebimento de energia externa;

3.1.1.4.4.2. Cabeamento de transmissão de energia;

3.1.1.4.4.3. Quadros de distribuição;

3.1.1.4.4.4. Cabos para conexões de rede;

3.1.1.4.4.5. Possuir múltiplas entradas independentes para fornecimento de energia elétrica. Cada entrada para fornecimento de energia elétrica deve ser capaz de isoladamente suportar a operação do data center;

3.1.1.4.4.6. Possuir múltiplas conexões independentes para acesso à Internet. Cada conexão para acesso à Internet deve ser capaz de isoladamente suportar a operação do data center.

3.1.1.5. A LICITANTE deve possuir ao menos dois SOCs de modo que a indisponibilidade de um deles não afete nenhum aspecto dos serviços prestados. Os

SOCs devem estar localizados no Brasil, em cidades diferentes e a no mínimo 50km de distância geodésica um do outro. Cada um deles deve atender aos seguintes requisitos mínimos:

3.1.1.5.1. Estar localizado em prédio comercial que:

3.1.1.5.1.1. Possua gerador de energia para as áreas privativas. O gerador deve ser acionado automaticamente em caso de falta de energia e fornecer energia estabilizada em até 2 minutos após a partida. Os geradores devem suportar a demanda das instalações por até 12 horas sem necessidade de reabastecimento.

3.1.1.5.1.2. Efetue registro dos visitantes com identificação individual e controle digital de entrada e saída.

3.1.1.5.1.3. Possua circuito interno de registro e gravação de imagem em todas as áreas de circulação;

3.1.1.5.1.4. Esteja localizado próximo a vias de grande circulação com acesso imediato a transportes públicos de mais de uma modalidade;

3.1.1.5.2. Funcione em regime 24 x7x365;

3.1.1.5.3. Possua sistema de refrigeração de conforto central.

3.1.1.5.4. Estar conectado aos Data Centers que hospedam os sistemas de suporte técnico, monitoramento, administração e gerenciamento através de múltiplas conexões de rede local ou WAN de forma que a falha de uma conexão isoladamente não afete o acesso aos mesmos;

3.1.1.5.5. Possuir estrutura central para visualização dos painéis dos sistemas de suporte técnico, monitoramento, administração e gerenciamento que permita que todos os profissionais visualizem eventos relevantes simultaneamente.

3.2. EQUIPE

3.2.1. A CONTRATADA deve fornecer pessoal necessário e tecnicamente habilitado à boa e integral execução dos serviços;

3.2.2. A CONTRATADA deve fornecer todos os materiais e serviços próprios e adequados à execução dos trabalhos, competindo-lhe ainda o fornecimento das demais utilidades relacionadas ao cumprimento do objeto deste edital;

3.2.3. A CONTRATADA deve retirar dos serviços qualquer empregado que, a critério do BANPARÁ, seja julgado inconveniente ao bom andamento dos trabalhos;

3.2.4. A CONTRATADA deve comunicar, imediatamente, por escrito quaisquer dificuldades encontradas pelos técnicos alocados para execução dos serviços que, eventualmente, possam prejudicar a boa e pontual execução dos trabalhos, sob pena de serem tais dificuldades consideradas inexistentes;

3.2.5. Comprovação de possuir no seu quadro permanente, no mínimo, profissionais com os certificados abaixo:

Certificação	**Quantidade de Profissionais**
ITIL Foundation Certified	02
PMP – Project Management Professional	01
Certificação emitida pela fabricante da solução(software) de Firewall/VPN ofertada	01
Certificação emitida pela fabricante da solução de IPS ofertada	01
Certificação emitida pela fabricante da solução de Gestão de Vulnerabilidades ofertada	01
Certificação emitida pela fabricante da solução de Filtro de E-mail ofertada	01
Certificação emitida pela fabricante da solução de Antivírus	01
Certificação na solução de Filtro de Web	01
Certificação na solução de Prevenção de perda de dados	01
Certificação na solução de gerenciamento de SIEM	01
Certificação na solução de proteção a ameaças avançadas e zero-day (Dia Zero)	01
Certificação na solução de Monitoramento e Proteção de Base de Dados	01

3.2.6. Comprovação de que o profissional é funcionário em regime CLT ou sócio, fornecendo cópia da carteira de trabalho ou Contrato/Estatuto Social da Empresa, com assinatura reconhecida em cartório competente.

3.2.7. Caso ocorra o desligamento de qualquer um dos profissionais exigidos no item 3.2.5, durante a vigência do contrato, a empresa deverá providenciar um substituto, com as mesmas certificações, no prazo máximo de 60 dias.

3.3. EXPERIÊNCIA

3.3.1. A LICITANTE deve possuir atestado(s) de capacidade técnica, focados em prestação de Serviços Gerenciados de Segurança, 24x7x365, onde são ou foram prestados pelo menos os seguintes serviços ou similares que compõem o objeto deste Edital: Firewall Próxima Geração e VPN, Prevenção de Intrusos, Gestão de Risco e Compliance, Gateway de E-mail e Web, Proteção das Estações de Trabalho e Servidores de Rede, Proteção Contra Vazamento e Integridade dos Dados, Gestão de Eventos e Incidentes, Proteção Contra Ameaças Dia Zero e Monitoramento e Proteção de Base de Dados conferido por empresas públicas ou privadas. O(s) atestado(s) deve(m) comprovar que a(s) rede(s) gerenciada(s) somam, pelo menos, 3.000 (três mil) hosts;

3.3.2. A LICITANTE deve ser parceiro qualificado pela(s) fabricante(s) pelo menos nas seguintes soluções que serão gerenciadas: Firewall Próxima Geração e VPN, Prevenção de Intrusos, Gestão de Risco e *Compliance*, *Gateway* de E-mail e Web, Proteção das Estações de Trabalho e Servidores de Rede, Proteção Contra Vazamento e Integridade dos Dados, Gestão de Eventos e Incidentes, Proteção Contra Ameaças Dia Zero e Monitoramento e Proteção de Base de Dados.

3.4. OUTRAS CARACTERÍSTICAS

3.4.1. Não será permitida a participação de consórcios e sub-locação de serviços em parte ou de modo global.

4. NMS (NÍVEL MÍNIMO DE SERVIÇO)

4.1. Os tempos máximos de resolução especificados nas tabelas 2 a 10 devem ser seguidos, sob pena de multa:

4.1.1. Firewall Próxima Geração e VPN

Atividade	Tempo de Resolução Máximo
Alteração e inclusão de regras	180 minutos após abertura de chamado, exceto quando for necessária uma janela de manutenção

Atividade	Tempo de Resolução Máximo
Alteração de configurações	180 minutos após abertura de chamado, exceto quando for necessária uma janela de manutenção
Atualização (implementação de patches e fixes)	48 horas após liberação do pacote pelo fabricante, condicionado à homologação pela CONTRATADA e liberação de janela de mudança pelo BANPARÁ
Início de atuação remota para resolução de problemas	180 minutos após abertura de chamado ou detecção pelo SOC
Início da atuação local para resolução de problemas e troca de equipamentos	24 horas após abertura de chamado ou detecção pelo SOC
Implementação de novos serviços ou dispositivos (VPN, placas de rede, etc.)	24 horas após abertura de chamado no Response Team
Relatório Periódico Técnico	Mensal
Relatório emergencial	24 horas após o evento, desde que solicitado pelo BANPARÁ

Tabela 2: NMS para serviço de Firewall Próxima Geração e VPN

4.1.2. Serviço de Prevenção de Intrusos

Atividade	Tempo de Máximo de Resolução
Alteração e inclusão de assinaturas de reconhecimento de ataques	180 minutos após a liberação do pacote de assinaturas pelo fabricante, condicionado à homologação pela CONTRATADA
Alteração de configurações	180 minutos após abertura de chamado, exceto quando for necessária uma janela de manutenção
Atualização (implementação de patches e fixes)	48 horas após liberação do pacote pelo fabricante, condicionado à homologação pela CONTRATADA e liberação de janela de mudança pelo BANPARÁ
Início de atuação remota para resolução de problemas	180 minutos após abertura de chamado ou detecção pelo SOC

Atividade	Tempo de Máximo de Resolução
Início da atuação local para resolução de problemas e troca de equipamentos	24 horas após abertura de chamado ou detecção pelo SOC
Relatório Periódico Técnico	Mensal
Relatório Emergencial	24 horas após o evento, desde que solicitado pelo BANPARÁ

Tabela 3: NMS para serviço de Prevenção de Intrusos

4.1.3. Serviço de Gestão de Risco e *Compliance*

Atividade	Tempo de Resolução Máximo
Atualização da Base de vulnerabilidades	180 minutos após a liberação do pacote de assinaturas pelo fabricante, condicionado à homologação pela CONTRATADA
Realização de scans para reporte de vulnerabilidades de alta criticidade.	A cada 72 horas
Realização de scans para reporte de vulnerabilidades de média e baixa criticidade.	Quinzenal
Alteração de configurações	180 minutos após abertura de chamado, exceto quando for necessária uma janela de manutenção
Atualização (implementação de patches e fixes)	48 horas após liberação do pacote pelo fabricante, condicionado à homologação pela CONTRATADA e liberação de janela de mudança pelo BANPARÁ
Início de atuação remota para resolução de problemas	180 minutos após abertura de chamado ou detecção pelo SOC
Início da atuação local para resolução de problemas e troca de equipamentos	24 horas após abertura de chamado ou detecção pelo SOC
Relatório Periódico Técnico	Mensal
Relatório emergencial	24 horas após o evento, desde que solicitado pelo BANPARÁ

Tabela 4: NMS para serviço de Gestão de Risco e Compliance

4.1.4. Serviço de Gateway de E-mail e Web

Atividade	Tempo de Resolução Máximo
Alteração e inclusão de regras (blacklist, whitelist, arquivos, etc.)	180 minutos após abertura de chamado, exceto quando for necessária uma janela de manutenção
Alteração de configurações	180 minutos após abertura de chamado, exceto quando for necessária uma janela de manutenção
Atualização do antivírus	60 minutos após a liberação do pacote pelo fabricante e homologação da CONTRATADA
Atualização (implementação de patches e fixes)	48 horas após liberação do pacote pelo fabricante, condicionado à homologação pela CONTRATADA e liberação de janela de mudança pelo BANPARÁ
Início de atuação remota para resolução de problemas	180 minutos após abertura de chamado ou detecção pelo SOC
Início da atuação local para resolução de problemas e troca de equipamentos	24 horas após abertura de chamado ou detecção pelo SOC
Relatório periódico técnico	Mensal
Relatório Emergencial	24 horas após o evento, desde que solicitado pelo BANPARÁ

Tabela 5: NMS para serviço de Gateway de E-mail e Web

4.1.5. Serviço de Gerenciamento de Proteção das Estações de Trabalho e Servidores de Rede

Atividade	Tempo de Resolução Máximo
Alteração e inclusão de regras	180 minutos após abertura de chamado, exceto quando for necessária uma janela de manutenção
Atualização do antivírus	Console: 60 minutos após a liberação do pacote pelo fabricante e homologação da CONTRATADA

Atividade	Tempo de Resolução Máximo
Atualização (implementação de patches e fixes)	48 horas após liberação do pacote pelo fabricante, condicionado à homologação pela CONTRATADA e liberação de janela de mudança pelo BANPARÁ
Início de atuação remota para varredura sob demanda	180 minutos após abertura de chamado
Início da atuação local para resolução de problemas	24 horas após abertura de chamado ou detecção pelo SOC
Troca de equipamentos	24 horas após abertura de chamado ou detecção pelo SOC
Relatório periódico técnico	Mensal
Relatório emergencial	24 horas após o evento, desde que solicitado pelo BANPARÁ

Tabela 6: NMS para serviço de Proteção das Estações de Trabalho e Servidores de Rede

4.1.6. Serviço de Gerenciamento de Proteção Contra Vazamento e Integridade dos Dados

Atividade	Tempo de Resolução Máximo
Alteração e inclusão de regras	180 minutos após abertura de chamado, exceto quando for necessária uma janela de manutenção
Alteração de configurações	180 minutos após abertura de chamado, exceto quando for necessária uma janela de manutenção
Atualização (implementação de patches e fixes)	48 horas após liberação do pacote pelo fabricante, condicionado à homologação pela CONTRATADA e liberação de janela de mudança pelo BANPARÁ
Início de atuação remota para resolução de problemas	180 minutos após abertura de chamado ou detecção pelo SOC
Início da atuação local para resolução de problemas	24 horas após abertura de chamado ou detecção pelo SOC
Troca de equipamentos	24 horas após abertura de chamado ou detecção pelo SOC
Relatório periódico técnico	Mensal

Atividade	Tempo de Resolução Máximo
Relatório emergencial	24 horas após o evento, desde que solicitado pelo BANPARÁ

Tabela 7: NMS para serviço de Proteção Contra Vazamento e Integridade dos Dados

4.1.7. Serviço de Gerenciamento de Gestão de Eventos e Incidentes

Atividade	Tempo de Resolução Máximo
Alteração e inclusão de regras	180 minutos após abertura de chamado, exceto quando for necessária uma janela de manutenção
Alteração de configurações	180 minutos após abertura de chamado, exceto quando for necessária uma janela de manutenção
Atualização (implementação de patches e fixes)	48 horas após liberação do pacote pelo fabricante, condicionado à homologação pela CONTRATADA e liberação de janela de mudança pelo BANPARÁ
Início de atuação remota para resolução de problemas	180 minutos após abertura de chamado ou detecção pelo SOC
Início da atuação local para resolução de problemas	24 horas após abertura de chamado ou detecção pelo SOC
Troca de equipamentos	24 horas após abertura de chamado ou detecção pelo SOC
Relatório periódico técnico	Mensal
Relatório emergencial	24 horas após o evento, desde que solicitado pelo BANPARÁ

Tabela 8: NMS para serviço de Proteção Contra Vazamento e Integridade dos Dados

4.1.8. Serviço de Gerenciamento de Proteção das Estações de Trabalho e Servidores de Rede

Atividade	Tempo de Resolução Máximo
Alteração e inclusão de regras	180 minutos após abertura de chamado, exceto quando for necessária uma janela de manutenção

Alteração de configurações	180 minutos após abertura de chamado, exceto quando for necessária uma janela de manutenção
Atualização (implementação de patches e fixes)	48 horas após liberação do pacote pelo fabricante, condicionado à homologação pela CONTRATADA e liberação de janela de mudança pelo BANPARÁ
Início de atuação remota para resolução de problemas	180 minutos após abertura de chamado ou detecção pelo SOC
Início da atuação local para resolução de problemas	24 horas após abertura de chamado ou detecção pelo SOC
Troca de equipamentos	24 horas após abertura de chamado ou detecção pelo SOC
Relatório periódico técnico	Mensal
Relatório emergencial	24 horas após o evento, desde que solicitado pelo BANPARÁ

Tabela 9: NMS para serviço de Proteção Contra Ameaças Dia Zero

4.1.9. Serviço de Gerenciamento de Monitoramento e Proteção de Base de Dados

Atividade	Tempo de Resolução Máximo
Alteração e inclusão de regras	180 minutos após abertura de chamado, exceto quando for necessária uma janela de manutenção
Alteração de configurações	180 minutos após abertura de chamado, exceto quando for necessária uma janela de manutenção
Atualização (implementação de patches e fixes)	48 horas após liberação do pacote pelo fabricante, condicionado à homologação pela CONTRATADA e liberação de janela de mudança pelo BANPARÁ
Início de atuação remota para resolução de problemas	180 minutos após abertura de chamado ou detecção pelo SOC
Início da atuação local para resolução de problemas	24 horas após abertura de chamado ou detecção pelo SOC

Troca de equipamentos	24 horas após abertura de chamado ou detecção pelo SOC
Relatório periódico técnico	Mensal
Relatório emergencial	24 horas após o evento, desde que solicitado pelo BANPARÁ

Tabela 10: NMS para serviço de Monitoramento e Proteção de Base de Dados

4.2. Em casos emergenciais, quando houver a paralisação nas atividades do negócio ou uma demanda de nível superior, o BANPARÁ poderá abrir chamados emergenciais, com o NMS diferenciado, conforme a tabela abaixo. O BANPARÁ designará 2 pessoas que poderão abrir chamados emergenciais. Poderão ser abertos, no máximo, 2 chamados emergenciais por mês.

4.2.1. Chamada Emergencial.

Atividade	Tempo de Resolução Máximo
Alteração e inclusão de regras	60 minutos após abertura de chamado, exceto quando for necessária uma janela de Manutenção.
Alteração de configurações	60 minutos após abertura de chamado, exceto quando for necessária uma janela de Manutenção
Alteração e inclusão de assinaturas de reconhecimento de ataques	60 minutos após a liberação do pacote de assinaturas pelo fabricante, condicionado à homologação pela CONTRATADA
Alteração de configurações	60 minutos após abertura de chamado, exceto quando for necessária uma janela de manutenção
Início de atuação remota para resolução de problemas	60 minutos após abertura de chamado

Tabela 11: NMS para serviços emergenciais

4.3. Os NMSs, especificados nas tabelas 2 a 11, podem ser revisados 1 (um) ano após a assinatura do contrato, caso o BANPARÁ entenda que os tempos aqui especificados não estão atendendo as suas necessidades, sujeito à aceitação da CONTRATADA.

5. DESCRIÇÃO DOS NÍVEIS DE SERVIÇOS REQUERIDOS

5.1. Para os serviços de Firewall Próxima Geração, VPN, Prevenção de Intrusos, Monitoramento e Proteção de Base de Dados que fazem parte do objeto deste Termo de Referência deverão ter:

5.1.1. Disponibilidade de serviço mensal de no mínimo 99,7% (noventa e nove vírgula sete por cento). Este percentual será calculado da seguinte forma:

5.1.1.1. Apura-se a quantidade de horas de indisponibilidade no mês;

5.1.1.2. Apura-se a quantidade de horas de disponibilidade do mês;

5.1.1.3. Subtrai-se o número de horas de disponibilidade no mês pelo número de horas de indisponibilidade no mês;

5.1.1.4. Divide-se o valor obtido no item anterior pelo número de horas de disponibilidade no mês;

5.1.1.5. Multiplica-se o valor obtido no item anterior por 100 (cem).

5.2. Para o serviço de Gateway de E-mail e Web que faz parte do objeto deste Termo de Referência deverá ter:

5.2.1. Disponibilidade de serviço mensal de, no mínimo, 98% (noventa e oito por cento). Este percentual será calculado da seguinte forma:

5.2.1.1. Apura-se o número de horas de indisponibilidade no mês;

5.2.1.2. Apura-se o número de horas de disponibilidade do mês;

5.2.1.3. Subtrai-se o número de horas de disponibilidade no mês pelo número de horas de indisponibilidade no mês;

5.2.1.4. Divide-se o valor obtido no item anterior pelo número de horas de disponibilidade no mês;

5.2.1.5. Multiplica-se o valor obtido no item anterior por 100 (cem).

5.3. Para os serviços de Gestão de Risco e Compliance, Proteção das Estações de Trabalho, Servidores de Rede, Proteção Contra Ameaças Dia Zero, Proteção Contra Vazamento e Integridade dos Dados, que fazem parte do objeto deste Termo de Referência deverão ter:

5.3.1. Disponibilidade de serviço mensal de, no mínimo, 95% (noventa e cinco por cento). Este percentual será calculado da seguinte forma:

5.3.1.1. Apura-se o número de horas de indisponibilidade no mês;

5.3.1.2. Apura-se o número de horas de disponibilidade do mês;

5.3.1.3. Subtrai-se o número de horas de disponibilidade no mês pelo número de horas de indisponibilidade no mês;

5.3.1.4. Divide-se o valor obtido no item anterior pelo número de horas de disponibilidade no mês;

5.3.1.5. Multiplica-se o valor obtido no item anterior por 100 (cem).

5.4. Não serão consideradas indisponibilidade as seguintes situações:

5.4.1. Falta de energia no local de instalação da solução;

5.4.2. Indisponibilidade da rede lógica à qual esteja instalado equipamento da solução;

5.4.3. Manutenções programadas pela CONTRATADA ou pelo BANPARÁ com aceite dado em documento pela parte requerida.

5.5. O tempo máximo de manutenções, por serviço gerenciado implantado, programadas pela CONTRATADA, não deverá ultrapassar 4 (quatro) horas mês e 24 (vinte e quatro) horas ano. Estes tempos referem-se a um equipamento ou conjunto de equipamentos de uma solução (Exemplo: cluster – dois ou mais equipamentos ou fail-over).

5.6. Todos os serviços cujos NMS (Nível Mínimo de Serviço) fazem parte do objeto deste Termo de Referência deverão ter meta de atendimento de, no mínimo, 95% (noventa e cinco por cento). Este percentual será calculado, por serviço, da seguinte forma:

5.6.1. Apura-se o número de chamados de serviço atendidos dentro do NMS no mês;

5.6.2. Apura-se o número de chamados de serviço atendidos fora do NMS no mês;

5.6.3. Subtrai-se o número de chamados do serviço atendidos dentro do NMS no mês pelo número de chamados do serviço atendidos fora do NMS no mês;

5.6.4. Divide-se o valor obtido no item anterior pelo número de chamados de serviço no mês;

5.6.5. Multiplica-se o valor obtido no item anterior por 100 (cem).

5.7. DESCONTOS PELO NÃO CUMPRIMENTO DOS SLAS ESPECIFICADOS E ATRASOS NA FASE DE IMPLANTAÇÃO:

5.7.1. Ao final do mês, será computado o percentual de atendimento ao SLA de cada serviço contratado, conforme definido no item 4 – Descrição dos Níveis de Serviço Requeridos.

5.7.2. Caso o nível de atendimento do SLA seja inferior a 95% (noventa e cinco por cento), será aplicado desconto de 15% (quinze por cento) na nota fiscal/fatura dos serviços;

5.7.3. Caso o percentual de atendimento esteja compreendido entre 95% e 96.99%, será aplicado desconto de 5% (cinco por cento) na nota fiscal/fatura dos serviços;

5.7.4. Caso o percentual de atendimento esteja compreendido entre 97% e 97.99%, será aplicado desconto de 3% (três por cento) na nota fiscal/fatura dos serviços;

5.7.5. Pelo fechamento não autorizado de chamados técnicos:

5.7.5.1. Os chamados abertos somente poderão ser fechados após autorização de funcionário designado pelo BANPARÁ. Caso haja fechamento de chamados, por parte da contratada, que não tenha sido previamente autorizado pelo BANPARÁ, será cobrada uma multa de 0,5% (zero vírgula cinco por cento) no valor mensal do serviço, por chamado fechado sem autorização, cumulativamente.

5.7.6. Pelo não cumprimento do índice de disponibilidade do serviço:

5.7.6.1. Será computado como indisponibilidade todo o tempo decorrido entre o início da interrupção do serviço e sua total recuperação;

5.7.6.2. Ao final do mês, será computado o tempo total de indisponibilidade do serviço, conforme definido no item 5 - DESCRIÇÃO DOS NÍVEIS DE SERVIÇOS REQUERIDOS, sendo cobrada uma multa de 0,5% (zero vírgula cinco por cento) no valor mensal do serviço por hora ou fração que exceder ao limite estabelecido para o serviço. Caso haja mais de um serviço em que o tempo total de disponibilidade ficou fora do limite estabelecido de tolerância, será aplicada, adicionalmente, multa de 1% (um por cento) no valor mensal do serviço, cumulativamente;

6. ESPECIFICAÇÕES TÉCNICAS

6.1. A Solução Integrada de Serviços Gerenciados de Segurança deverá englobar alocação de equipamentos, produtos, peças e softwares necessários à perfeita execução das atividades e atendimento às especificações técnicas durante o prazo de vigência, incluindo manutenção e atualização dos produtos e softwares utilizados e monitoramento de segurança em regime 24x7 (vinte e quatro horas por dia, sete dias por semana).

6.2. A prestação dos serviços será baseada no modelo de remuneração em função dos resultados apresentados, em que os pagamentos serão feitos após mensuração e verificação de métricas quantitativas e qualitativas, contendo indicadores de desempenho e metas, com Nível Mínimo de Serviço (NMS) definido em contrato, de modo a resguardar a eficiência e a qualidade na prestação dos serviços. Os níveis mínimos de serviços contratados, presentes no Nível Mínimo de Serviço destas especificações técnicas, serão registrados, monitorados e comparados às metas de desempenho e qualidade estabelecidas, em termos de prazo e efetividade, condição fundamental para efetuar os pagamentos previstos.

6.3. O modelo de prestação de serviço conterá, ainda, processos de trabalho que especificam como os serviços serão prestados, incluindo atividades a serem demandadas pelo BANPARÁ, tais como abertura de chamados técnicos para resolução de problemas e de consulta a informações, e aquelas a serem desenvolvidas periodicamente pela CONTRATADA, tais como análise de vulnerabilidades de segurança e monitoração das ferramentas utilizadas nos serviços.

6.4. Os serviços constantes no objeto deste Termo de Referência estão subdivididos conforme a Tabela 12 que segue:

Item	Descrição	Quantidade	Meses
1	Serviço de Firewall Próxima Geração e VPN	1	48
1.1	Inicialização dos Serviços da Solução de Firewall Próxima Geração e VPN	1	
2	Serviço de Prevenção de Intrusos	1	48
2.1	Inicialização do Serviço de Prevenção de Intrusos	1	
3	Serviço de Gestão de Risco e Compliance	1	48
3.1	Inicialização do Serviço de Gestão de Risco e Compliance	1	
4	Serviço de Gateways de Email e Web	1	48
4.1	Inicialização do Serviço de Gateways Email e Web	1	
5	Serviços de Proteção das Estações de Trabalho e Servidores de Rede	1	48
5.1	Inicialização dos Serviços de Proteção das Estações de Trabalho e Servidores de Rede	1	
6	Serviço de Proteção Contra Vazamento e Integridade dos Dados	1	48
6.1	Inicialização dos Serviços de Proteção Contra Vazamento e Integridade dos Dados	1	
7	Serviço de Gestão de Eventos e Incidentes	1	48
7.1	Inicialização do Serviço de Gestão de Eventos e Incidentes	1	
8	Serviço de Proteção Contra Ameaças Dia Zero	1	48
8.1	Inicialização do Serviço de Proteção Contra Ameaças Dia Zero	1	
9	Serviço de Monitoramento e Proteção de Base de Dados	1	48
9.1	Inicialização do Serviço de	1	

	Monitoramento e Proteção de Base de Dados		
10	**Treinamentos**	**Quantidade**	
10.1	Treinamento Firewall Próxima Geração e VPN	1	
10.2	Treinamento Prevenção de Intrusos	1	
10.3	Treinamento Gestão de Risco e Compliance	1	
10.4	Treinamento Gateway de Email e Web	1	
10.5	Treinamento Proteção das Estações de Trabalho e Servidores	1	
10.6	Treinamento Proteção contra Vazamento e Integridade dos Dados	1	
10.7	Treinamento Gestão de Eventos e Incidentes	1	
10.8	Treinamento Proteção Contra Ameaças Dia Zero	1	
10.9	Treinamento Monitoramento e Proteção de Base de Dados	1	
11	Monitoração e Administração de Segurança	1	
12	Serviços Técnicos Especializados	4.000 horas	

Tabela 12: Escopo de Serviços – Detalhamento

6.4.1. O Item 1 refere-se ao Serviço de "***Firewall* Próxima Geração e VPN**", provido por um Cluster de, pelo menos **2 (dois)** equipamentos e **1 (um)** equipamento de "spare" para o caso de substituição quando necessário e **1 (um)** *appliance* (Físico ou virtual) para gerenciamento destes equipamentos, capazes de regular o tráfego de dados entre as distintas redes do Banpará e impedir a transmissão e recepção de tráfego nocivo ou não autorizado de uma rede para outra. Os equipamentos deverão implementar tecnologias de filtro de pacotes S*tateful Inspection*, utilizando mecanismos de verificação de tráfego segundo tabela de estado de conexões. Oportunamente, o serviço deverá contar com um equipamento instalado no *Site* Primário do Banpará e outro de maneira similar no *Site* Secundário do Banpará, em Belém, sem descaracterizar a instalação realizada no primeiro, mantendo também as mesmas características de proteção em ambos os *Sites*. Além disso, os equipamentos do cluster deverão ser capazes de implementar recursos de criptografia para tunelamento em redes inseguras de comunicação, tal como a Internet, por meio de redes privadas virtuais (VPN),

garantindo confidencialidade, autenticação e integridade necessárias para a segurança do tráfego de dados do Banpará;

6.4.2. O item 2 destina-se à prestação dos "**Serviços de Prevenção de Intrusos**" no Banpará, providos por no mínimo **1(um)** appliance (Físico ou virtual) para gerenciamento e **2 (dois)** equipamentos do tipo appliance (físicos) com capacidade para no mínimo **6 (seis)** segmentos de rede e capazes de identificar, prevenir e bloquear tentativas de intrusão e atividades maliciosas de rede entre os diversos segmentos de rede do Banpará em Belém, incluindo o acesso à Internet, à rede MPLS e à rede de contingência VPN. Deverão, ainda, implementar tecnologias de detecção e bloqueio de intrusão por meio de assinaturas e por análise de comportamento, com topologia IPS in-line em modo pass-through/fail-over. Deverão ser capazes de interromper tráfego de rede que tenha potencial para causar danos às informações ou ainda o consumo desnecessário de recursos de rede. Os equipamentos serão alocados no Datacenter Principal e secundário do Banpará em Belém, mantendo as mesmas características de proteção em ambos os Datacenters;

6.4.3. O item 3 consiste em "**Serviços de Gestão de Risco e *Compliance***" providos por no mínimo **2 (dois)** appliances (Fisícos ou virtuais) e licenciamento para 3000 hosts e licenciamento para software capaz de detectar, inventariar e avaliar vulnerabilidades encontradas nas aplicações WEB, sistemas e recursos de TI e ainda na solução de segurança fornecida, especialmente quanto ao impacto no ambiente computacional e ao risco inerente à segurança das informações custodiadas. Deverá englobar instalação de agentes e validação de conformidade por meio de monitoração periódica e por demanda, segundo as diretrizes de segurança a serem definidas em conjunto com o Banpará.

6.4.4. O item 4 refere-se aos Serviços de "***Gateways de Email e Web***" responsável pela liberação e bloqueio de acessos feitos pelos usuários da rede corporativa à websites e assemelhados, conforme política de acesso à Internet definida pelo Banpará. O serviço será provido por no mínimo **5 (cinco)** *appliances* (Físicos ou Virtuais) e licenciamento para no mínimo **3000 (Três mil) usuários únicos** onde **2 (dois)** em cluster para o serviço de *Gateway* de *Web*, os equipamentos em par deverão ter seus elementos instalados sendo utilizadas tecnologias de balanceamento ativo-ativo ou de tolerância a falhas ativo-passivo. O serviço deverá prover tecnologias de proxy transparente e cache. Ademais, o item refere-se também à solução de bloqueio de e-mails não solicitados pelos usuários do Banpará, capazes de impactar a produtividade de seus colaboradores e degradar o desempenho dos sistemas e redes corporativas, além de potencialmente comprometer a segurança das informações por eles custodiadas. Consistirá também em **2 (dois)** *appliances* (Físicos ou

virtuais) em cluster para o serviço de *Gateway* de Email. Será admitida a configuração do balanceamento por meio de prioridades em registros do tipo MX no DNS do Banpará. Este serviço deverá suportar funções de relay SMTP e antispam, dotado de tecnologias de filtro de reputação, bloqueio por listas negras e quarentena por usuário. Conterá também **1 (um)** *appliance* (Virtual ou Físico) para servidor de relatórios e **licenciamento para 3000 (três mil) usuários únicos**, proporcionando maior auditabilidade, rastreabilidade e visibilidade das ações nestes serviços.

6.4.5. O Item 5 trata dos "**Serviços de Proteção das Estações de Trabalho e Servidores de Rede**" consistirá em no mínimo **2 (dois)** *appliances* (Físicos ou Virtuais) para gerenciamento dos **3000 (três mil)** *endpoints* licenciados que serão responsáveis por proteger o ambiente computacional do Banpará contra *malwares* (Trojans, Virus, *Worms*, *Spywares* e demais ameaças), ataques, pacotes indesejados e controle dos dispositivos inseridos nas estações de Trabalho. A solução deverá ser capaz de oferecer uma proteção otimizada e avançada antivírus aos seus desktops e servidores virtualizados para no mínimo **500 (quinhentos)** *endpoints* virtualizados licenciados. A Solução deverá possuir capacidade de informar sites maliciosos e até autorizar e/ou bloquear o acesso e possuir centro de inteligência capaz de informar reputação de arquivos.

6.4.6. O Item 6 trata dos "**Serviço de Proteção Contra Vazamento e Integridade dos Dados**" que deverá fornecer pelo menos (**4 quatro)** *appliances* e 3000 mil licenças responsáveis por proteger as informações e a propriedade intelectual produzida pelos colaboradores do Banpará. A solução deverá proteger padrões de documentos a serem estipulados em conjunto com a equipe do Banpará e locais os quais responsáveis por armazenar informações confidenciais e críticas para o negócio. Locais com informações críticas deverão ser protegidos e capaz de garantir a confidencialidade e integridade da informação. Oportunamente, poderão ser instalados sensores de captura de tráfego de rede e bloqueio no Datacenter Secundário, sem que se desfaça a proteção do site Primário.

6.4.7. O Item 7 trata dos "**Serviços de Gestão de Eventos e Incidentes**" que deverá fornecer no mínimo **1 (um)** *appliance* (Físico ou Virtual) com capacidade para pelo menos **5000 eventos por segundo**, responsável por coletar, armazenar, processar, monitorar e correlacionar logs de ativos e servidores de rede do Banpará, bem como da própria solução de segurança fornecida, de modo a executar ações reativas e proativas, como envio de notificações e alertas aos administradores da rede do Banpará e da própria contratada. Os elementos a serem monitorados englobará toda a Solução a ser fornecida. Não fará parte do escopo dos serviços o monitoramento de desktops, estações de videoconferência, laptops,

smartphones, dispositivos *wireless*, impressoras e equipamentos de controle de acesso de pessoas às instalações do Banpará.

6.4.8. O Item 8 trata dos "**Serviços de Proteção Contra Ameaças Dia Zero**" a ser fornecido com no mínimo **1 (um)** *appliance* (obrigatoriamente físico) responsável por receber arquivos desconhecidos e analisá-los no ambiente do Banpará, em Belém, com capacidade de simular as imagens dos Sistema Operacionais utilizadas no ambiente computacional do Banpará e executar os arquivos com a intenção de simular se o mesmo tem capacidade maliciosa podendo vir a causar perda de informações ou indisponibilidade no ambiente do Banpará.

6.4.9. O item 9 trata dos "**Serviços de Monitoramento e Proteção de Base de Dados**" deverá ser fornecido por *software* licenciado para no mínimo **15 (quinze)** instâncias de banco de dados e será responsável pelo monitoramento dos acessos às Bases de dados do BANPARÁ e suas informações, realizados por aplicações e usuários com capacidade para fornecer trilha completa de auditoria, visibilidade e controle completo das conexões as bases de dados protegendo-as de ataques e acessos indevidos, bloqueando ataques e encerrando sessões indevidas, além de corrigir vulnerabilidades, através de patches virtuais, o que torna desnecessária janela de manutenção para correção, aumentando assim a disponibilidade das bases de dados;

6.4.10. O item 10 trata dos "**Treinamentos"** a serem prestados ao Banpará com vistas à transferência de conhecimento, compreendendo as tecnologias envolvidas nos serviços contratados dos itens 6.4.1 a 6.4.9, assim como capacitação nos produtos e softwares utilizados para atender aos requisitos destas especificações técnicas. As atividades de treinamento serão realizadas para no mínimo 6 e no máximo 8 **(oito) servidores** da equipe do Banpará e deverão possuir carga horária de no **mínimo 40 (quarenta) horas**, sendo obrigatório que o **fabricante da solução ministre** a capacitação **com conteúdo de curso oficial**, emitindo ao final o certificado de conclusão de curso para cada um dos cursos ministrados.

6.4.11. O item 12 trata de **Serviços Técnicos Especializados** em segurança da informação, com métrica baseada em horas de serviço, compreendendo a execução de atividades de elaboração de pareceres e planos, análise de ambiente e de ativos, auditoria forense, mudança de endereço de unidades do Banpará (aspectos de segurança) e alteração de arquitetura do ambiente computacional e da infraestrutura de segurança do Banpará. Consiste em atividades a serem demandadas por meio da celebração prévia de ordens de

serviço, com total de horas definido previamente, de comum acordo entre o Banpará e a contratada, cujo pagamento será efetivado somente após entrega de relatório de prestação de serviços e recebimento por parte do Banpará.

6.4.12. Todos os *cluster's* formados devem funcionar no modo ativo/ativo, para todos os demais serviços que exigirem a alocação de equipamentos, produtos, peças ou softwares em modo cluster, ou seja, em alta disponibilidade, ficará facultado à contratada escolher qual a melhor modalidade para a configuração da solução, seja tecnologia de balanceamento ativo-ativo ou de tolerância a falhas ativo-passivo. Em todos os casos devem ser respeitadas as capacidades mínimas requeridas para os serviços a serem entregues.

6.4.13. Caso a CONTRATADA opte por fornecer *appliances* virtuais, onde esta utilização não é vedada a *appliances* físicos (*Firewall* Próxima Geração e VPN, Prevenção de Intrusos e Serviço de Proteção Contra Ameaças Dia Zero, exceto *appliances* de gerenciamento) por motivos de performance e topologia, deverá fornecer *hardware* compatível com as exigências mínimas exigidas pela FABRICANTE para utilização deste *appliance* virtualizado, bastando para isso comprovar na proposta técnica e comercial que hardware oferecido atende aos requisitos básicos do sistema que será virtualizado.

6.4.14. O desenho da topologia será entregue no ato da vistoria prévia, mediante entrega de Termo de Confidencialidade e Sigilo do licitante devidamente assinado pelo representante legal da empresa, com firma reconhecida.

7. ESPECIFICAÇÕES TÉCNICAS MÍNIMAS

São apresentadas, a seguir, especificações técnicas mínimas dos serviços a serem ofertados referentes aos itens 1 a 12 do objeto. Os termos "possui", "permite", "suporta" e "é" implicam no fornecimento de todos os elementos necessários à adoção da tecnologia ou funcionalidade citada. O termo "ou" implica que a especificação técnica mínima dos serviços pode ser atendida por somente uma das opções. O termo "e" implica que a especificação técnica mínima dos serviços deve ser atendida englobando todas as opções.

Todos os equipamentos, produtos, peças ou softwares necessários à prestação dos serviços deverão ser novos e de primeiro uso e não constar, no momento da apresentação da proposta, em listas de *end-of-sale*, *end-of-support* ou *end-of-life* do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante. Já os softwares comerciais deverão, ainda, ser instalados em sua versão mais

atualizada, e estar cobertos por contratos de suporte a atualização de versão do fabricante durante toda a vigência do respectivo serviço. Da mesma maneira, todo o hardware a ser utilizado na prestação dos serviços deverá estar coberto por garantia do fabricante.

O conjunto dos requisitos especificados em cada item poderá ser atendido por meio de composição com os outros equipamentos, produtos, peças ou softwares utilizados no atendimento aos demais itens, desde que isso não implique em alteração da topologia ou na exposição de ativos a riscos de segurança e mantenham-se todos os módulos propostos integrados entre si, ou seja, trocando informações entre os módulos deste termo de Referência, simplificando a gestão e minimizando os riscos a segurança do BANPARÁ.

Ademais, todos os componentes necessários à prestação dos serviços deverão ser integráveis entre si, mantendo-se como uma única solução sem restrições aos requisitos constantes nestas especificações técnicas, e aos elencados do parque computacional do BANPARÁ.

7.1. SERVIÇO DE FIREWALL PRÓXIMA GERAÇÃO E VPN

7.1.1. Características gerais da Solução:

7.1.1.1. Toda Solução de segurança proposta deverá ser fornecida por um único fabricante de modo que tanto o suporte a solução quanto as funcionalidades sejam inteiramente integradas e gerenciadas através de uma única console de gerenciamento.

7.1.2. Características de hardware por equipamento (*Appliance*)

7.1.2.1. Throughput mínimo de 30 (trinta) Gbps para firewall.

7.1.2.2. Capacidade para suportar no mínimo o *throughput* 14 (quatorze) Gbps de tráfego inspecionado.

7.1.2.3. *Throughtput* mínimo de 11 (onze) Gbps para VPN IPSec.

7.1.2.4. *Throughtput* mínimo de 3 (três) Gbps para inspeção SSL (AES-256).

7.1.2.5. Possibilitar 20 (vinte) milhões de conexões simultâneas.

7.1.2.6. Possibilitar 6 (seis) Milhões de conexões simultâneas inspecionadas.

7.1.2.7. Possibilitar 25 (Vinte cinco) Milhões de pacotes por segundo.

7.1.2.8. Possibilitar 200.000 (duzentas mil) conexões novas estabelecidas por segundo.

7.1.2.9. Possibilitar até 100 (cem) virtualizações/contexto

7.1.2.10. As seguintes interfaces deverão estar livres para produção em cada equipamento de firewall:

7.1.2.10.1. No mínimo, 4 (quatro) interfaces de 10 (dez) Gigabit Ethernet (padrão SFP+). As interfaces de rede devem ser todas frontais.

7.1.2.10.2. No mínimo 12 (doze) interfaces Gigabit Ethernet 1000Mbps para cabeamento de cobre.

7.1.2.11. Deve suportar a definição de VLAN no firewall conforme padrão IEEE 802.1q e ser possível criar interfaces ou subinterfaces lógicas associadas a VLANs e estabelecer regras de filtragem (Stateful Firewall) entre elas.

7.1.2.12. Possuir LED indicativo de on/off.

7.1.2.13. Possuir 2 (duas) fontes de alimentação internas, independentes, hot swappable e redundantes, com tensão de entrada de 120V a 240V AC (manual ou automática)

7.1.3. Características do software de firewall e VPN

7.1.3.1. Deve ser configurável para operar em uma das seguintes funções de forma exclusiva:

7.1.3.1.1. *Firewall*/VPN (layer 3);
7.1.3.1.2. IPS mode (layer 2);
7.1.3.1.3. *Firewall* (layer 2);

7.1.3.2. Deve suportar até 20.000 (vinte mil) túneis VPN;

7.1.3.3. Sem restrições de número máximo de máquinas protegidas.

7.1.3.4. Possuir sistema operacional customizado especificamente para funções de firewall.

7.1.3.5. Prover mecanismo de conversão de endereços NAT (*Network Address Translation*), de forma a possibilitar que:

7.1.3.5.1. Possa realizar NAT estático (1-1), dinâmico (N-1), NAT pool (N-N) e NAT condicional, com o objetivo de possibilitar que um endereço tenha mais de um NAT dependendo da origem, destino ou porta.

7.1.3.6. Permitir que redes ou faixas de endereços IP reservados acessem a Internet a partir de um ou mais endereços IP públicos (Dynamic NAT).

7.1.3.7. Permitir o registro de eventos de NAT com as informações de endereço interno, endereço público, data e hora do evento, portas de origem e destino.

7.1.3.8. Permitir que as regras de NAT sejam configuradas diretamente no appliance independente de qual política será aplicada e permitir a criação de NAT seja também possível via política.

7.1.3.9. Permitir que a definição da tradução do NAT para o IP externo seja configurável através de elementos/objetos, interface ou um endereço de IP específico.

7.1.3.10. Permitir a definição de NAT default nas propriedades do firewall.

7.1.3.11. Deverá contemplar as seguintes funcionalidades:
7.1.3.11.1. AntiSpam;
7.1.3.11.2. Antivírus;
7.1.3.11.3. Multilink;
7.1.3.11.4. Cluster;
7.1.3.11.5. Balanceamento de carga entre servidores;
7.1.3.11.6. Controle de aplicação;
7.1.3.11.7. QoS.

7.1.3.12. A solução deve ter a capacidade de realizar inspeção avançada de pacotes (*Deep Packet Inspection*), e tal funcionalidade deve ser ajustável de forma granular para tráfegos específicos.

7.1.3.13. A solução deve ter a capacidade de identificar as aplicações trafegadas pela rede.

7.1.3.14. Suporte de inspeção multi-camada, permitindo combinar inspeção do tráfego ao nível da aplicação, inspeção stateful e análise de pacotes para que possa seguir as conexões e poder identificar se um pacote é parte de uma conexão estabelecida ou não.

7.1.3.15. Suporte nativo para a integração de serviços de diretório tais como MS Active Directory, LDAP v3, Novell eDirectory, RADIUS e TACACS +.

7.1.3.16. Habilidade para autenticar os usuários através de um portal.

7.1.3.17. Recurso de qualidade de serviço (QoS) deve prover ao menos as seguintes funcionalidades:

7.1.3.17.1. Garantia / reserva de banda;
7.1.3.17.2. Limite de utilização da banda;
7.1.3.17.3. Prioridade do tráfego;
7.1.3.17.4. DSCP (Differentiated Services Coe Point).

7.1.3.18. As configurações dos perfis QoS devem ser aplicadas por interface.

7.1.3.19. Capacidade de uso concorrente de múltiplos provedores WAN (Multi-Link), suportando tráfego de entrada, saída e entre localidades.

7.1.3.20. Deve prover agentes especificos para no mínimo os seguintes protocolos:

7.1.3.20.1. FTP
7.1.3.20.2. H.323
7.1.3.20.3. HTTP
7.1.3.20.4. HTTPS
7.1.3.20.5. IMAP4
7.1.3.20.6. MGCP
7.1.3.20.7. MS RPC
7.1.3.20.8. NetBios Datagram
7.1.3.20.9. Oracle SQL Net

7.1.3.20.10. POP3
7.1.3.20.11. RSH
7.1.3.20.12. RTSP
7.1.3.20.13. SCCP
7.1.3.20.14. SIP
7.1.3.20.15. SMTP
7.1.3.20.16. SSH
7.1.3.20.17. SunRPC
7.1.3.20.18. TCP proxy
7.1.3.20.19. TFTP

7.1.3.21. Possibilitar o controle do tráfego para os protocolos TCP, UDP e ICMP baseados nos endereços de origem e destino, bem como no serviço utilizado em uma comunicação.

7.1.3.22. Na instalação de regras/politicas as conexões existentes deverão ser mantidas sem perda das conexões ativas.

7.1.3.23. Prover mecanismo contra ataques de falsificação de endereços (IP *Spoofing*) por meio do qual permite-se habilitar o seu uso baseado na topologia.

7.1.3.24. Suportar *anti-spoofing* (sem uso de ACLs) para endereços IPv4 e IPv6.

7.1.3.25. Prover mecanismo contra ataques de negação de serviço (DoS) e SYN *Flood*, repassando somente as conexões estabelecidas entre os segmentos.

7.1.3.26. Suportar o protocolo DHCP no modo relay sendo esse configurado por interface.

7.1.3.27. Integração com MIBs que possam ser compiladas para o sistema de gerenciamento SNMP.

7.1.3.28. Suportar a configuração de agregação de interfaces, conforme padrão IEEE 802.3ad.

7.1.3.29. Suportar inspeção stateful de tráfego IPv4 e Ipv6.

7.1.3.30. Suportar a criação de regras IPv4 e Ipv6.

7.1.3.31. Possibilitar implementação de firewall em modo transparente ou em modo gateway (roteado).

7.1.3.32. Possuir funcionalidade nativa para captura de pacotes.

7.1.3.33. Sistema operacional deverá ser customizado pelo próprio fabricante do firewall para garantir segurança e melhor desempenho ao firewall, permitindo o monitoramento de recursos no *appliance*.

7.1.3.34. Deve permitir a criação de rotas estáticas e suportar OSPF ou BGP.

7.1.3.35. A solução de Firewall deve funcionar em cluster do tipo ativo-passivo ou ativo-ativo com balanceamento interno, ou seja, sem a necessidade de balanceador externo.

7.1.3.36. Os firewalls deverão ser configurados em modo ativo-ativo ou ativo-passivo e no caso de falha em um dos nós, o(s) remanescente(s) deverá(ão) assumir o controle automaticamente.

7.1.3.37. Na ocorrência de falhas, as conexões existentes em um firewall deverão ser mantidas pelo(s) outro(s) sem perdas destas conexões, não acarretando interrupções no tráfego da rede e nem redução de desempenho da solução.

7.1.3.38. Na configuração de alta-disponibilidade todas as configurações e estados de conexões devem ser replicados automaticamente entre os firewalls do cluster.

7.1.3.39. No caso de falha de um dos nós, as conexões ativas (IPSEC-VPN inclusive) devem continuar funcionando por meio do(s) outro(s) firewall(s) do cluster. Não poderão haver perdas de conexões ativas através do cluster, mesmo que estas passem por NAT ou VPN.

7.1.3.40. Capacidade de suportar até 16 nós em um mesmo cluster a fim de prover eficiência e disponibilidade do ambiente.

7.1.3.41. Os membros do cluster deverão suportar a convivência de versões distintas de firmware suportando no mínimo revisão X+2.

7.1.3.42. As atualizações dos membros do cluster podem ser feitas de forma independentes, garantindo a disponibilidade total do ambiente no momento da atualização e permitindo que essa ação possa ser executada a qualquer momento do dia.

7.1.3.43. Os membros do cluster poderão diferir de modelos, permitindo assim a utilização de caixas de diferentes modelos em um mesmo cluster.

7.1.3.44. Permitir a criação de VPN site-to-site e client-to-site.

7.1.3.45. Possuir compatibilidade com o padrão IPSEC, de acordo com as RFCs 2401 e RFCs 2403 a 2411, de modo a estabelecer canais de criptografia com outros produtos que também suportem tal padrão.

7.1.3.46. Fornecer criptografia e autenticação de pacotes IP com chaves de criptografia de 3DES/AES, no mínimo, de forma a possibilitar a criação de canais seguros ou IPSEC VPNs.

7.1.3.47. Suportar as topologias comuns de rede como Estrela, Hub and Spoke, Full Mesh.

7.1.3.48. A configuração de túneis VPN deverá suportar as seguintes configurações através de múltiplos links:

7.1.3.48.1. Ativo - Passivo
7.1.3.48.2. Ativo - Ativo
7.1.3.48.3. Link aggregation

7.1.3.49. Deve suportar os seguintes protocolos para VPN:

7.1.3.49.1. IKEv1;
7.1.3.49.2. IKEv2;

7.1.3.50. Deve suportar as seguintes criptografias para VPN:

7.1.3.50.1. AES-128;
7.1.3.50.2. AES-256;

7.1.3.50.3. AES-GCM-128;
7.1.3.50.4. AES-GCM-256;
7.1.3.50.5. Blowfish;
7.1.3.50.6. DES;
7.1.3.50.7. 3DES.

7.1.3.51. Deve suportar os seguintes grupos DH (Diffie-Hellman) para VPN:

7.1.3.51.1. 1;
7.1.3.51.2. 2;
7.1.3.51.3. 5;
7.1.3.51.4. 14;
7.1.3.51.5. 19;
7.1.3.51.6. 20;
7.1.3.51.7. 21.

7.1.3.52. Deve suportar os seguintes métodos de autenticação para VPN:

7.1.3.52.1. RSA;
7.1.3.52.2. DSS;
7.1.3.52.3. ECDSA;
7.1.3.52.4. pre-shared keys;
7.1.3.52.5. XAUTH;
7.1.3.52.6. EAP.

7.1.3.53. Suporte aos seguintes algoritimos para VPN:

7.1.3.53.1. AES-XCBC-MAC;
7.1.3.53.2. MD5;
7.1.3.53.3. SHA-1;
7.1.3.53.4. SHA-2-256;
7.1.3.53.5. SHA-2-512;

7.1.3.54. Habilidade de detecção e bloqueio de aplicação das seguintes formas:

7.1.3.54.1. Categoria
7.1.3.54.2. Grupo de Usuário

7.1.3.54.3. Usuário
7.1.3.54.4. IP origem
7.1.3.54.5. Zona
7.1.3.54.6. Porta
7.1.3.54.7. Interface
7.1.3.54.8. Protocolo

7.1.3.55. Suporte de bloqueio de no minímo 1000 aplicações distribuidas nos seguintes grupos de categoria:

7.1.3.55.1. Chat
7.1.3.55.2. Discussion Forum
7.1.3.55.3. Entertainment
7.1.3.55.4. File Sharing
7.1.3.55.5. Mail
7.1.3.55.6. Media
7.1.3.55.7. Miscellaneous
7.1.3.55.8. Office
7.1.3.55.9. P2P
7.1.3.55.10. Reference
7.1.3.55.11. Remote Control
7.1.3.55.12. Social Networking
7.1.3.55.13. Statistics
7.1.3.55.14. Storage
7.1.3.55.15. Tunneling

7.1.3.56. A Solução deve ser capaz de bloquear técnicas avançadas de evasão.

7.1.3.57. A capacidade de detectar a evasão deve ser capaz de analisar os fluxos de dados a fim de identificar o tráfego malicioso por meio da reconstrução do tráfego.

7.1.3.58. Ter a capacidade de realizar inspeção avançada de pacotes (*Deep Packet Inspection*) em todas as sessões de rede, independentemente do protocolo para detectar, identificar e relatar atividades e conteúdo suspeitos.

7.1.4. Características comuns de administração, gerenciamento e auditoria quanto a configuração, administração e gerenciamento dos firewalls e seus clusters.

7.1.4.1. Disponibilizar, por meio de interface serial ou das interfaces de rede, a configuração e o gerenciamento dos firewalls por linha de comando CLI (emulação de terminal Telnet ou SSH), via Web (HTTP ou HTTPS) ou cliente próprio.

7.1.4.2. Possuir criptografia na comunicação por meio de protocolo seguro.

7.1.4.3. Prover mecanismos de restrição de acesso remoto através de filtros de usuário/senha.

7.1.4.4. Prover meios para criar, modificar e excluir (além do padrão de fábrica) novos usuários e grupos administradores, pelo menos 03 (três), com diferentes níveis de acesso e funções (ex.: acesso total, leitura e escrita, somente leitura e outros níveis).

7.1.4.5. Permitir a conexão simultânea de vários usuários administradores. O acesso simultâneo destes não deverá comprometer a base de dados.

7.1.4.6. Permitir a instalação na configuração de alta-disponibilidade por tolerância a falhas, na qual:

7.1.4.6.1. Deverão ser configurados em modo ativo-ativo ou ativo-passivo e no caso de falha de um dos módulos de Gerenciamento Centralizado, o(s) remanescente(s) deverá(ão) assumir todas as funcionalidades de administração dos firewalls e seus clusters gerenciados.

7.1.4.6.2. Os softwares utilizados para acessar as gerências e realizar tarefas administrativas (GUI clients) deverão ser compatíveis com o sistema operacional Linux, MacOS e Windows.

7.1.4.7. Licenciamento e o software não devem limitar o número de objetos, regras de segurança, NAT, endereços IP e usuários.

7.1.4.8. A console gráfica deve fornecer, pelo menos, as seguintes opções de gerenciamento:

7.1.4.8.1. Gerenciamento remoto de múltiplos firewalls simultaneamente, sem a necessidade de se executar várias consoles gráficas.

7.1.4.8.2. Permitir a criação de regras centralizadas, de forma que possam ser aplicadas a diversos firewalls de maneira automática.

7.1.4.8.3. Possibilitar o gerenciamento (incluindo a criação, alteração, monitoração e exclusão) de objetos de rede. Deverá ainda permitir detectar se e onde, na base de regras, está sendo utilizado determinado objeto de rede. Os tipos de objetos deverão permitir especificar de forma distinta grupos e objetos de rede e serviços, diferenciando-os e agrupando-os conforme suas características ou descrição de maneira a permitir o reaproveitamento dos mesmos em diferentes políticas.

7.1.4.8.4. Possibilitar o gerenciamento (incluindo a criação, alteração, monitoração e exclusão) de regras de acesso no módulo de firewall, de forma individual para cada firewall ou generalizada em todos os módulos de firewall administrados.

7.1.4.8.5. As regras de acesso no módulo de firewall devem, no mínimo, definir ações como:

a) Allow (permitir);
b) Discard (descartar);
c) Refuse (recusar).

7.1.4.8.6. Suportar agrupamento lógico de objetos ("*object grouping*") para criação de regras de filtragem.

7.1.4.8.7. Possibilitar a especificação de política por tempo, ou seja, permitir a definição de regras para um determinado horário ou período (dia, mês, dia da semana e hora).

7.1.4.8.8. Possibilitar configurar, de forma gráfica, a solução de Firewall provida pelo fabricante da solução.

7.1.4.8.9. Possuir ferramenta de análise de consistência das regras para evitar conflitos lógicos entre novas regras e as existentes.

7.1.4.8.10. Permitir a reutilização de objetos lógicos em várias políticas de Segurança.

7.1.4.8.11. Permitir o retorno emergencial às configurações anteriores dos dispositivos para a necessidade de recuperação de falhas ("Rollback de configuração").

7.1.4.8.12. Deve fornecer proteção contra falha no caso de aplicação de regras mal formadas a fim de realizar a recuperação de forma automática ("Rollback") caso o dispositivo perca conectividade com a plataforma de gerência.

7.1.4.8.13. Permitir distribuição centralizada de pacotes de atualização e que essa seja realizada sem a interrupção do funcionamento dos equipamentos de firewall.

7.1.4.8.14. Permitir testar a conectividade dos equipamentos gerenciados.

7.1.4.8.15. Suportar configuração das funcionalidades de alta disponibilidade dos dispositivos físicos.

7.1.4.8.16. Registrar em log de auditoria as ações dos usuários administradores.

7.1.4.8.17. Fornecer as informações detalhadas em real time (tempo-real) ou com o menor atraso possível, bem como relatórios e logs detalhados contendo, no mínimo:

a) Data e horário de acesso;
b) Recursos acessados por máquina;
c) Estatísticas de uso;
d) Conexões;
e) VPNs IPSEC negociadas;
f) Carga de utilização do sistema;
g) Estado de cada um dos equipamentos de firewall.

7.1.4.8.18. Fornecer as estatísticas dos principais (esse podendo ser ajustado para ex.: 5 principais, 10 principais, etc.) em real time (tempo-real) ou de um período específico possibilitando a geração automática de relatórios de no mínimo:

a) Aplicações em uso;
b) Ataques;
c) Usuários;
d) Ações;
e) Protocolos IP;
f) Origem;
g) Destino;
h) Localidade.

7.1.4.8.19. Permitir a geração de relatórios e gráficos a partir dos registros de eventos e logs dos firewalls gerenciados.

7.1.4.8.20. Possibilitar a monitoração de toda a comunicação realizada ou bloqueada através do módulo de firewall gerenciado, além de todas as ocorrências de mudanças nas suas configurações e demais aspectos importantes para auditoria do módulo de firewall.

7.1.4.8.21. Permitir o armazenamento e recuperação, por meio de protocolo criptografado, dos logs e eventos dos firewalls gerenciados em máquinas remotas e servidores de consolidação de logs ou permitir o armazenamento e recuperação via Syslog.

7.1.4.8.22. Permitir a geração de relatórios e gráficos a partir dos registros de eventos e logs dos firewalls gerenciados.

7.1.4.8.23. Possibilitar a aplicação remota de correções e atualizações para os módulos de firewall descritos anteriormente. No caso de configurado em cluster não deverá haver indisponibilidade do ambiente, ou seja, a atualização deve ocorrer de forma transparente.

7.1.4.8.24. Possibilitar a movimentação de objetos já usados em regras entre abas utilizando o conceito de drag-and-drop

7.1.4.8.25. Possuir suporte ao protocolo SNMP v3.

7.1.4.8.26. Permitir a verificação da utilização ("hit counts") de cada regra. Para cálculo deve ser possível determinar o período e no caso de regras usadas em múltiplos firewalls deve ser possível estipular qual firewall será alvo da contagem.

7.1.4.8.27. Possuir capacidade de carregar qualquer backup realizado anteriormente pelo sistema automático de backup.

7.1.4.8.28. Prover mecanismo de realização automática de backup de toda a configuração do Equipamento de segurança, incluindo os módulos de firewall e a própria solução de gerenciamento.

7.1.4.8.29. Permitir a criação de tarefas agendas para no mínimo as seguintes operações:

a) Aplicação de política;

b) *Export* dos logs;

c) *Archive* dos logs;

7.1.4.8.30. Prover integração com a solução de proteção de estações para permitir uma informação contextualizada do usuário final e do host utilizado por eles.

7.1.4.8.31. Prover integração com a solução de proteção contra ameaças dia-zero, permitindo o envio de arquivos suspeitos para análise e posterior remediação

7.1.4.8.32. Prover integração com Centro de Inteligência do próprio fabricante para informação de reputação de Endereços IP’s maliciosos e hash de arquivos.

7.2. SERVIÇO DE PREVENÇÃO DE INTRUSOS

7.2.1. Características Gerais da Solução:

7.2.1.1. A solução de IPS deve ser composta pelo fornecimento de no mínimo **1 (um)** appliance (Físicos ou Virtuais) para gerenciamento e **2 (dois)** appliances (Físicos) para os sensores com suporte a pelo menos 6 (seis) segmentos de rede com velocidade 1 Gbps com garantia, suporte técnico do fabricante e todos os recursos licenciados pelo período de 48 (quarenta e oito) meses.

7.2.1.2. Baseado em *Appliance Box* suportando montagem em *rack* (bastidor) de 19" (dezenove polegadas), com utilização de 2-RU (duas unidades de bastidor) de altura;

7.2.1.3. Baseado em arquitetura específica e desenvolvido, tanto software quanto hardware, para a funcionalidade única, exclusiva e específica de *Network Intrusion Prevention*, não sendo um equipamento de uso geral e/ou multifuncional (UTM – *Unified Threat Management*), tal como: Chassi Servidor (*Server Chassis*), Estação de Trabalho (Desktop) e/ou Equipamento Blade;

7.2.1.4. Suportar fonte de energia para Corrente Alterna ou Alternada (AC – *Alternating Current*);

7.2.1.5. Suportar fonte de energia com chaveamento automático e capacidade de operação em 100V à 240V (50/60Hz) em Corrente Alterna ou Alternada (AC – *Alternating Current*) substituível;

7.2.1.6. Suportar cabos elétricos com conectores de 3 (três) pinos cobertos fêmea (padrão IEC320-C13) e 3 (três) pinos macho plugue aterrado (padrão NEMA 5-15P).

7.2.1.7. Suportar, de forma homogênea e heterogênea, os seguintes modos de operação em um único equipamento: SPAN, Inline (*Fail-Open* e *Fail-Close*) e Grupo de Interfaces (*Port Clustering*);

7.2.1.8. Suportar instalação sem necessidade de reconfiguração de roteadores e switches, quanto no modo de operação *Inline Mode*;

7.2.1.9. Suportar monitoração e proteção de segmentos de rede em modo transparente e operação na camada 2 (Layer-2) do modelo OSI (*Open System Interconnection*);

7.2.1.10. Suportar instalação Inline Mode sem bloqueio para ataques, isto é, quando instalado em Inline Mode o equipamento pode ser configurado para não bloquear ataques específicos ou todos os ataques, apenas alertando-os;

7.2.1.11. Suportar inspeção de tráfego em ambiente com roteamento assimétrico e links agregados;

7.2.1.12. Suportar configuração flexível de "*inline-forward*" (Layer-2) para tráfego que ultrapasse a análise de tráfego agregado ("*over-subscription*") suportado pelo equipamento;

7.2.1.13. Suportar atualização de software e políticas sem necessitar da reinicialização do equipamento, onde não há paralisação do monitoramento de tráfego, e consequentemente detecção e bloqueio de ataques, durante o processo de atualização.

7.2.2. Sistema de Prevenção de Intrusos – Características para Appliances

7.2.2.1. Suportar análise de tráfego agregado de no mínimo 3 (três) Gbps, sem utilização de agregador de tráfego ou equipamento externo para balanceamento de tráfego;

7.2.2.2. Suportar taxa de no mínimo 5.000.000 (cinco milhões) conexões concorrentes e taxa de no mínimo 200.000 (duzentas mil) novas conexões TCP por segundo;

7.2.2.3. Suportar taxa de SYN Cookie de no mínimo 1.500.000 (Um milhão e quinhentos mil) pacotes TCP SYN por segundo com tamanho de 64 (sessenta e quatro) bytes;

7.2.2.4. Suportar desempenho de no máximo 100 µs (cem microssegundos) de latência para tráfego de pacotes UDP;

7.2.2.5. Permitir análise de tráfego HTTPS (HyperText Transfer Protocol Secure) no mesmo equipamento de IPS, isto é, conexões seguras com criptografia SSL (Secure Sockets Layer) em servidores WEB, para no mínimo servidores IIS e Apache, utilizando certificados PKCS12 (extensões ".pkcs12", ".p12", ou ".pfx"), nas versões SSLv2 e SSLv3/TLS e com codificações RC4, DES, 3DES e AES;

7.2.2.6. Suportar 1.000 (mil) certificados importados para análise de trafego SSL (Secure Sockets Layer);

7.2.2.7. Possuir 12 (doze) interfaces 1Ge (Gigabit Ethernet) Fast Ethernet para cabeamentos Cobre (1000BASE-T);

7.2.2.8. Possuir 2 (duas) interfaces 10GigE(Gigabit Ethernet)/1GigE (Gigabit Ethernet) SFP+;

7.2.2.9. Possuir capacidade de expansão para 8 portas SFP+/SFP 10 GigE ou 1 GigE sem a necessidade de troca do equipamento.

7.2.2.10. Possuir 1 (uma) interface 1Ge (Gigabit Ethernet), para cabeamentos Cobre (10BASE-T/100BASETX/1000BASE-T), exclusiva e dedicada para gerência;

7.2.2.11. Possuir 1 (uma) interface serial (padrão RS-232C) exclusiva e dedicada para console.

7.2.3. Características de Detecção de Ataques:

7.2.3.1. Suportar análise e decodificação de no mínimo 190 (cento e noventa) protocolos de rede, entre a camada 2 (Layer-2) e camada 7 (Layer-7) do modelo OSI (Open System Interconnection), permitindo detecção e bloqueio de ataques;

7.2.3.2. Suportar identificação de ataques para protocolos de rede independente das portas de comunicação utilizadas para, no mínimo, os protocolos: DNS, FTP, HTTP, POP3 e SMTP;

7.2.3.3. Suportar tanto a análise *Stateful Inspection*, mantendo-se o estado das sessões monitoradas, quanto a *Stateless Inspection*;

7.2.3.4. Suportar identificação passiva de sistemas operacionais (*Passive OS Fingerprint*) para sistemas monitorados em segmentos protegidos;

7.2.3.5. Suportar análise de tráfego na direção servidor-cliente, isto é, ataques originados externamente e direcionados à clientes e/ou usuários internos ("*Client-Side Attacks*" ou "*Drive-by Attacks*");

7.2.3.6. Suportar detecção e bloqueio de ataques direcionados à servidores de aplicação WEB (*WEB Application*), através de tecnologia heurística, isto é, detecção heurística e bloqueio de ataques SQL *Injection*;

7.2.3.7. Suportar inteligência sobre ataques baseada em tecnologia em nuvem, permitindo proteção em tempo real para ataques de *malwares* sem necessidade de atualização e/ou existência de assinaturas;

7.2.3.8. Permitir obtenção de informações detalhadas sobre ataques de no mínimo: Reputação de Arquivo (*File Reputation*), Reputação de Endereço IP (*IP Reputation*), Reputação de Aplicação e Protocolo (*Application and Protocol Reputation*) e Localização geográfica (País), tanto do endereço IP de origem quanto de destino;

7.2.3.9. Suportar detecção heurística de atividades de agentes (zumbis) internos que pertençam a Botnet;

7.2.3.10. Suportar administração, configuração e manutenção de controle de limites de taxa de transferências (Rate Limiting), permitindo controle e bloqueio de tráfego indesejado;

7.2.3.11. Suportar detecção e bloqueio de *Shellcodes* através de tecnologia patenteada, permitindo que instruções de computador sejam examinadas – para a presença de uma instrução de chamada do sistema – e revisadas – para a presença de um conjunto de instruções de "*decoder*" (descodificador).

7.2.3.12. Suportar as categorias de ataques e tipos de ameaças, para no mínimo:

7.2.3.12.1. Reconnaissance: Brute Force, Host Sweep, OS Fingerprinting, Port Scan e Service Sweep;
7.2.3.12.2. Exploits: Arbitrary Command Execution, Backdoor, Bot, Buffer Overflow, Denial of Service, DDoS Agent Activity, Code/Script Execution, Evasion Atempt, Privileged Access, Probe, Protocol Violation, Remote Access, Shellcode Execution, Trojan, Virus, Read Exposure, Worms e Write Exposure;
7.2.3.12.3. Volume DoS: Statistical Deviation e Over Threshold;
7.2.3.12.4. Policy Violations: Audit, Command Shell, Covert Channel, Non-standard Port, Phising, PuP (Potential Unwanted Program), Restricted Access, Restricted Application, Sensitive Content e Unauthorized IP.

7.2.3.13. Suportar detecção e bloqueio de ataques do tipo *Denial-of-Service* (DoS) e *Distributed Denial-of-Service* (DDoS) de forma nativa, para no mínimo:

7.2.3.13.1. Assinaturas para detecção e bloqueio de ataques através de vulnerabilidades DoS, conforme padrões de mercado e definidos por entidades independentes (*Computer Emergency Response Team* e *Common Vulnerability and Exposures*), para no mínimo: CA-1996-26, CA-1997-28, CA-1998-13, CVE-1999-0015, CVE-1999-

0016, CVE-1999-0128, CVE-1999-0153, CVE-1999-0258, CVE-1999-0345, CVE-1999-0969, CVE-2000-0305, CVE-2004-0230, CVE-2004-0790, CVE-2005-0688 e CVE-2005-0048;

7.2.3.13.2. Assinaturas para detecção e bloqueio de atividades de agentes (zumbis) DDoS, conforme padrões de mercado e definidos por entidades independentes (*Computer Emergency Response Team e Common Vulnerability and Exposures)*, para no mínimo: CA-1999-17, CA-2000-01, CVE-2000-0138, IN-99-07, IN-2000-01 e IN-2000-05;

7.2.3.14. Detecção e bloqueio baseado em modo aprendizagem (*Learning Mode*), através de anomalias estatísticas (*Statistical Anomalies*) e desequilíbrio de volume de tráfego, que permite utilização de perfil de tráfego tanto de longo quanto de curto prazo, para *Flood* (Volume) *DoS Attacks*, conforme padrões de mercado e definidos por entidades independentes (*Computer Emergency Response Team* e *Common Vulnerability and Exposures*), para no mínimo: CA-1996-21, CA-1996-01, CA-1998-01 e CVE-2002-1712;

7.2.3.15. Detecção e bloqueio baseados em *SYN Cookie* (*SYN Proxy*), que permita utilização de uma "*secret key*" juntamente ao ISN (*Initial Sequence Number*) – nos pacotes de resposta TCP (SYN+ACK) às requisições de conexão TCP (SYN) – como parte integrante do processo de "3-*way handshake*".

7.2.3.16. Políticas de Firewall camada 3 (Layer 3), que permitam no mínimo:

7.2.3.16.1. Filtros de origem e destino por: país (Geo-localização), nome (DNS), endereço IPv4, bloco de endereços IPv4, rede ou grupo de redes;

7.2.3.16.2. Filtros de aplicação: aplicação, grupo de aplicações, porta de comunicação customizada, serviço ou grupo de serviços;

7.2.3.16.3. Filtro de tempo efetivo (temporizador): período de tempo finito, período de tempo recorrente ou grupo de períodos de tempo recorrente;

7.2.3.16.4. Filtro de resposta: bloqueio (drop) e negação (deny), tanto para *Stateful* quanto para *Stateless*, e ignorar.

7.2.3.17. Limite de conexões, que permite definição de valores "*threshold*" para limitar o número de conexões que podem ser estabelecidas de/para uma máquina, através de no mínimo: Protocolos, Reputação, Geolocalização e Conexões ativas ou taxa de conexão.

7.2.3.18. Gerenciamento de tráfego (Traffic Managment), que permita adequação do perfil de tráfego desejado de um segmento de rede à uma necessidade específica, através de no mínimo: Rate Limiting, DiffServ e 802.1p;

7.2.3.19. Proteção de servidores DNS (*Domain Name Service*) contra ataques - com ou sem a presença de endereços IP forjados (*IP Spoofing*) – e que permita utilizar-se apenas do protocolo TCP para resolução de nomes (*name lookup*/resolve), não permitindo a utilização do protocolo UDP para esta finalidade.

7.2.3.20. Suportar detecção e bloqueio de tráfego de aplicações *Instant Messenger* e P2P (*Peer-to-Peer*), para no mínimo: AOL *Instant Messenger*, Ares, Azureus, Bearshare, Bittorrent, Blubster, DirectConnect, eDonkey, eMule, Enppy, ICQ, FileNara, Gnucleus, Gnutella, Grokster, Groove, JAP Anonymizer, Kazaa, Limewire, Morpheus, MSN Messenger, Mutella, MyNapster, Mxie, OpenLITO, Overnet, Phex, Piolet, RockItNet, Shareaza, Skype, SoulSeek, Swapper, Xolox, WinMX e Yahoo! Messenger;

7.2.3.21. Suportar detecção e bloqueio de ataques através de túneis IPv6, para no mínimo: IPv4 in IPv4, IPv4 in IPv6, IPv6 in IPv4 e IPv6 in IPv6;

7.2.3.22. Suportar detecção e bloqueio de ataques através de segmentos encapsulados para no mínimo: ECLB (*EtherChannel Load Balancing*), Double VLAN, GPRS (*General Packet Radio Service*) Tunneling Protocol, GRE (*Generic Routing Encapsulation*), IEEE 802.1Q, IEEE 802.1Q-in-Q, Jumbo Frames, MPLS (Multi Protocol Label Switching), SSL (Secure Sockets Layer), Stacked VLAN, VLAN Bridging (*Pairing*) e VLAN Bridging (*Pairing*) em STP (*Spanning Tree Protocol*);

7.2.3.23. Suportar detecção de ataques ARP (Address Resolution Protocol) Spoofing.

7.2.4. Características de respostas da solução:

7.2.4.1. Suportar TCP Reset para: Origem do ataque, Destino do ataque e Origem e destino do ataque.

7.2.4.2. Suportar ICMP Host Unreachable;

7.2.4.3. Suportar bloqueio (*Drop*) de pacotes;

7.2.4.4. Suportar aplicação, extensão e remoção de quarentena (*IPS Quarantine*) sob demanda;

7.2.4.5. Suportar captura de pacotes para análise de evidências em formato LIBPCAP (*Library for Packet Capture*);

7.2.4.6. Suportar envio de SNMP para as versões SNMPv1, SNMPv2c e SNMPv3;

7.2.4.7. Suportar envio de e-mail.

7.2.5. Características de Gerenciamento da Solução:

7.2.5.1. Possuir políticas baseadas em assinaturas recomendadas pelo fabricante para bloqueio (*Recommended for Blocking*), as quais são baseadas nas recomendações provenientes de equipe de pesquisa do fabricante;

7.2.5.2. Suportar console de gerência no modelo "Agent-less", isto é, não há necessidade de instalação de software de console de gerenciamento;

7.2.5.3. Suportar customização de "*Dashboards*" para visualização resumida de eventos;

7.2.5.4. Suportar operação com Sistema Gerenciador de Banco de Dados Relacional (SGBDR – *Relational Database Management System* ou RDBMS) que utilize linguagem de pesquisa declarativa SQL (*Structured Query Language*);

7.2.5.5. Suportar modos heterogêneos de atualização para no mínimo:

7.2.5.5.1. Online: automática e/ou manual de conteúdo de segurança e produto através da Internet, podendo ser realizada sem interferência do usuário;

7.2.5.5.2. Offline: automática e/ou manual de conteúdo de segurança e produto através de pacotes de atualização importados pela gerência, sem conexão com a Internet.

7.2.5.6. Suportar administração, configuração e manutenção de contas de acesso de usuários e administradores através de autenticação:

7.2.5.6.1. LOCAL: usuários e administradores cadastrados na gerência, permitindo definir políticas de composição de senhas;

7.2.5.6.2. LDAP: usuários e administradores importados e integrados com o Windows AD (Active Directory);

7.2.5.6.3. RADIUS: usuários e administradores importados e integrados com servidor RADIUS.

7.2.5.7. Suportar atribuição de perfis para usuário e administradores, para no mínimo: Administrador IPS (Intrusion Prevention System), Operador NOC (Network Operation Center), Gerador de relatórios, Administrador de sistema, Super usuário e Perfil nulo.

7.2.5.8. Suportar customização da console de gerência para exibir logo da empresa e mensagem aos usuários e administradores no momento da autenticação;

7.2.5.9. Suportar criação de ACL (Access Control List – Lista de Controle de Acesso), especificando quais endereços IP terão permissão de comunicação com a gerência;

7.2.5.10. Suportar comunicação entre gerência e equipamento criptografada, com as seguintes características:

7.2.5.10.1. SSL (Secure Sockets Layer) com RC4 e MD5 (Message-Digest algorithm 5);

7.2.5.10.2. SSL (Secure Sockets Layer) com MD5 (Message-Digest algorithm 5);

7.2.5.10.3. SSL (Secure Sockets Layer) de criptografia de 128-bit.

7.2.5.11. Suportar SNMPv3 (*Simple Network Management Protocol Version* 3) de 56-bit DES (*Data Encryption Standard*) e MD5 (*Message-Digest Algorithm* 5);

7.2.5.12. Suportar integração, através de SNMPv3, com solução de Sistema de Gerenciamento de Rede (NMS – *Network Management System*);

7.2.5.13. Fornecer arquivo MIB (SNMPv3) para integração com solução de Sistema de Gerenciamento de Rede (NSM – *Network Management System*);

7.2.5.14. Suportar processamento de 2.160.000 (dois milhões, cento e sessenta mil) eventos (alertas) por dia, recebidos dos equipamentos.

7.2.6. Características de Integração com a solução de Gestão de Vulnerabilidades e Riscos.

7.2.6.1. Suportar integração com a solução de Gestão de Vulnerabilidades e Riscos, não sendo permitida a utilização de um único equipamento para suportar tanto funcionalidade de IPS quanto de Gestão de Vulnerabilidades e Riscos, para no mínimo:

7.2.6.1.1. Solução Open-source.

7.2.6.2. Suportar modos heterogêneos de integração para no mínimo:

7.2.6.2.1. Automática: Importação automática e agendada de resultados de análise de vulnerabilidades;
7.2.6.2.2. Manual: Importação manual de resultados de análise de vulnerabilidades.

7.2.6.3. Suportar demonstração de informações detalhadas dos ativos de rede, tanto para origem quanto para o destino, através de correlação de ataques e vulnerabilidades, para no mínimo: Sistema operacional do ativo de rede, Service Pack do ativo de rede, Portas de comunicação abertas e ativas no ativo de rede, Protocolos de comunicação disponíveis no ativo de rede, Serviços disponíveis no ativo de rede, Lista de vulnerabilidades do ativo de rede.

7.2.6.4. Suportar demonstração de informações sobre a relevância do ataque, isto é, quanto gerado um alerta de um ataque, é informado se o destino (alvo) é vulnerável, ou não, àquele ataque, sendo este alerta relevante ou não.

7.2.6.5. Suportar integração ativa à solução de análise de vulnerabilidades, ou seja, independente da importação do resultado de *scan* da solução de análise de vulnerabilidades, a solução IPS deve realizar acesso e consulta ao banco de dados da solução de análise de vulnerabilidades.

7.2.7. Características de integração a solução de *Endpoint* e gerência de ameaças:

7.2.7.1. Suportar integração ativa a solução de gerencia de *endpoint*, ou seja, devem estar disponíveis informações da estação origem ou destino do evento.

7.2.7.2. A console de gerência do IPS deve trazer no mínimo as seguintes informações do *Endpoint* afetado pelo evento: Sistema Operacional, últimos 10 eventos detectados na solução de IPS de Host e últimos 10 eventos detectados na solução de Antivirus.

7.3. Solução de Gestão de Risco e Compliance

7.3.1. Características Gerais da solução:

7.3.1.1. A solução de Gestão de Vulnerabilidades e Riscos deve ser composta pelo fornecimento de pelo menos 2 appliances (Físico ou Virtuais) com garantia, suporte técnico do fabricante e todos os recursos licenciados pelo período de 48 (quarenta e oito) meses;

7.3.1.2. Deve possuir um "engine" de varredura de vulnerabilidades de alto desempenho, em plataforma 64 bits;

7.3.1.3. Deve ter a capacidade de detectar vulnerabilidades em aplicações baseadas em Web, bases de dados, aplicações comerciais, sistemas operacionais e dispositivos de rede;

7.3.1.4. Possuir ferramenta de gestão completa sob o ciclo de vida das vulnerabilidades, que seja capaz de identificar a causa raiz da vulnerabilidade e avaliar o impacto de novas ameaças;

7.3.1.5. Identificar e correlacionar as ameaças, além de avaliar o potencial risco de novas ameaças através da correlação de eventos de ativos e informações de vulnerabilidades;

7.3.1.6. A solução não deve ser baseada somente em agente, sendo capaz de executar de forma eficiente varredura da rede a fim de identificar ativos e determinar seu sistema operacional e as vulnerabilidades que nele possam existir;

7.3.1.7. Atualizar automaticamente a biblioteca de verificação com cobertura 24/7;

7.3.1.8. Fornecer conjuntos de vulnerabilidades predefinidos com base em padrões de conformidade populares;

7.3.1.9. Suportar o armazenamento seguro de credenciais, para uso em varreduras autenticadas, usando-as para se autenticar em sistemas Windows, UNIX ou qualquer ativo de infraestrutura, tais como os dispositivos de rede;

7.3.1.10. Permitir a modificação de métricas por administradores para atender aos requisitos específicos do negócio;

7.3.1.11. A descrição de vulnerabilidade deve possuir no mínimo os seguintes detalhes:

7.3.1.11.1. Nome;

7.3.1.11.2. Nível de Risco;

7.3.1.11.3. Intrusiva (sim / não);

7.3.1.11.4. Descrição;

7.3.1.11.5. Recomendação;

7.3.1.11.6. Número CVE;

7.3.1.11.7. SANS / FBI referência Top 20 (se aplicável);

7.3.1.12. Suportar Varreduras baseados em grupos de ativos;

7.3.1.13. Suportar Varreduras com credenciais e sem credenciais;

7.3.1.14. Possibilidade de integração com os métodos de autenticação existentes, incluindo LDAP, Active Directory e SecureID/RADIUS;

7.3.1.15. Disponibilizar informações sobre o andamento detalhado de Varredura;

7.3.1.16. Suportar a escrita de scripts personalizados para testes sistemas proprietários e legados;

7.3.1.17. Suportar a realização de varreduras com prioridade, permitindo que verificações importantes possam acontecer a toda velocidade, enquanto outras análises sejam executadas mais lentamente;

7.3.1.18. Facilitar a criação de verificações personalizadas para procurar vulnerabilidades únicas ou mandatos de conformidade corporativa;

7.3.1.19. Realizar verificações direcionadas (controlo de um conjunto específico de vulnerabilidades);

7.3.1.20. Especificar o escopo de credenciais usando o endereço IP, nome DNS, nome NETBIOS, ou credencial padrão;

7.3.1.21. Fornecer técnicas de discovery para analisar clientes wireless, pontos de acesso, switches e roteadores;

7.3.1.21.1. Prover integração nativa com a solução de Gestão de Eventos e Incidentes, alimentando os hosts existentes e as vulnerabilidades associadas a cada um deles como forma de enriquecer o processo de correlação de eventos;

7.3.1.22. Deve permitir o gerenciamento dos scanners a partir de uma console única centralizada.

7.3.1.23. Fornecer painéis pré-construídos que atendam as seguintes informações:

7.3.1.23.1. Vulnerabilidades mais críticas;
7.3.1.23.2. Sistemas operacionais mais críticos;
7.3.1.23.3. Lista de vulnerabilidades por Gravidade;
7.3.1.23.4. Percentagem vulnerabilidade Gravidade;
7.3.1.23.5. Gráficos de tendência.

7.3.1.24. Fornecer trilha de auditoria detalhada para acessos e ações de usuários;

7.3.1.25. Permitir a aferição do risco de unidades de negócios e regiões;

7.3.1.26. A descrição detalhada da vulnerabilidade deve incluir passos recomendados para remediação e, se possível, todas as recomendações provenientes da base de conhecimento on-line e um link ao artigo adequado;

7.3.1.27. Fornecer painéis executivos que incluam pontuações de segurança da informação;

7.3.1.28. Fornecer relatórios executivos para análise de medidas globais de segurança, bem como análise de tendências de curto e longo prazo;

7.3.1.29. Gerar relatórios flexíveis à categorização dos dados por ativo ou por rede;

7.3.1.30. Produzir relatórios detalhados que classifiquem as vulnerabilidades por risco;

7.3.1.31. Os dashboards e relatórios gerados devem fornecer links para descrições detalhadas das vulnerabilidades encontradas. Cada vulnerabilidade deve estar correlacionada com padrão de referência, como: CVE, SANS, IAVA;

7.3.1.32. Apoiar o uso de filtros para selecionar e organizar os resultados nos relatórios;

7.3.1.33. Capacidade de enviar eventos para solução de gerenciamento centralizado de segurança, onde são gerados Dashboards e relatórios, e que podem ser consumidos por outras soluções de segurança desse mesmo fabricante.

7.3.1.34. Deve incluir mecanismos para varredura de hosts, bancos de dados e aplicações web, incluindo a detecção de vulnerabilidades em AJAX e Web 2.0;

7.3.1.35. Deve oferecer a varredura "segura" de sistemas SCADA – Supervisory Control And Data Acquisition;

7.3.1.36. Deve ter a capacidade de atualizar automaticamente a tabela de ativos do Gerenciador de Incidentes Eventos e Segurança, preenchendo informações sobre os serviços e as vulnerabilidades encontradas no(s) ativo(s) analisado(s);

7.3.1.37. Deve ter a capacidade de correlacionar os eventos baseados nos sistema operacional, Porta, Protocolo, Banners e Vulnerabilidades;

7.3.1.38. Capacidade de verificações de vulnerabilidades: de uma forma não invasiva, invasiva, por tipo de risco, categoria e CVE;

7.3.1.39. Deve ter a capacidade de verificação de vulnerabilidades em ambiente Windows deve incluir: detecção de hot fixes, *service packs*, registros, *backdoors*, trojans, peer-to-peer e Antivírus;

7.3.1.40. Deve a ter a capacidade de integrar com solução de DLP (Data Loss Prevention) e tomar uma ação conforme política pré-estabelecida;

7.3.1.41. A Solução deve ter recursos que permitam a detecção automática das famílias de vulnerabilidades do documento OWASP Top 10 (https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project);

7.4. Serviço de Gateways de Email e Web

7.4.1. Características mínimas da Solução de Gateway de Email:

7.4.1.1. Deverá ser fornecido com no mínimo **2 (dois)** appliances (Físicos ou Virtuais) para análise de e-mails e **1 (um)** appliance para a Quarentena (Físicos ou Virtuais) com suporte a **3000 (três mil)** caixas postais de E-mail, não considerando grupos ou listas de distribuição como caixas de e-mail;

7.4.1.2. **Da Plataforma:**

7.4.1.2.1. Ser uma solução MTA (*Mail Transfer Agent*) completa com suporte ao protocolo SMTP.

7.4.1.2.2. Deve ser capaz de filtrar o tráfego de correio, bloqueando a entrada de vírus, *spyware*, *worm*s, *trojans*, *SPAM*, *phishing*, e-mail marketing, e-mail adulto ou qualquer outra forma de ameaça virtual.

7.4.1.2.3. Deve permitir alta disponibilidade das funções de filtragem, de maneira assegurar que o serviço de correio nunca pare por falha da solução.

7.4.1.2.4. Suportar no mínimo 10.000 conexões simultâneas e ser capaz de processar 160.000 mensagens por hora ou mais.

7.4.1.2.5. A solução deve ser apresentada na forma de *appliance* (conjunto de máquina, sistema operacional e sistema aplicativo), através de servidores de rack 19", com no máximo 2U de altura, dispondo de, no mínimo: 4 interfaces de rede gigabit, 6 núcleos de processamento (sem considerar hyper trading), 8GB de memória RAM e 4 discos SAS de 300Gb, em RAID10.

7.4.1.2.6. A solução deve ser apresentada na forma de *appliance* virtual (conjunto de máquina virtual, sistema operacional e sistema aplicativo), com *hardware* virtualizado na plataforma VMWare.

7.4.1.3. **Da Alta Disponibilidade:**

7.4.1.3.1. O cluster deve poder operar com máquinas em racks e em datacenters distantes e, ainda assim, manter sua integridade.

7.4.1.3.2. O cluster deve poder operar em clusters de virtualização em datacenters distantes e, ainda assim, manter sua integridade.

7.4.1.3.3. O cluster deve poder ser formado por *appliances* físicos e *appliaces* virtuais, de forma mista.

7.4.1.3.4. Possuir capacidade de replicação automática das configurações e balanceamento de carga através de DNS.

7.4.1.4. **Do Gerenciamento:**

7.4.1.4.1. Possuir interface web de administração segura HTTPS.

7.4.1.4.2. Suportar o gerenciamento e replicação de políticas do cluster de forma centralizada.

7.4.1.4.3. Possuir níveis granulares de administração da interface web, permitindo que se crie perfis diferentes de administradores.

7.4.1.4.4. Permitir que se crie sub-organizações, com grupos de usuários, para que um administrador somente gerencie uma sub-organização.

7.4.1.4.5. Possuir opção de acesso remoto, direto do fabricante do produto, para eventual manutenção, ficando a critério do administrador sua ativação ou não.

7.4.1.4.6. Prover acesso, via linha de comando, via protocolo seguro (SSH), para identificação de problemas e criação de *scripts*.

7.4.1.4.7. Prover funcionalidade de backup e restauração das configurações da solução.

7.4.1.4.8. Prover funcionalidade de armazenagem e retorno de, no mínimo, as 5 (cinco) últimas mudanças de configuração, sem interrupção (restauração de back-up) do serviço.

7.4.1.4.9. Opção de *feedback* para engenharia do produto, através da interface gráfica reportar mensagem de feedback, solicitar aprimoramento ou *feature*.

7.4.1.4.10. Barra de status com as seguintes informações em tempo real:

7.4.1.4.10.1. Quantidade de mensagens trafegando no cluster

7.4.1.4.10.2. Quantidade de conexões no cluster

7.4.1.4.10.3. Quantidade de mensagens em quarentena

7.4.1.4.10.4. Quantidade de mensagens trafegando por agente de filtro do cluster

7.4.1.4.10.5. Quantidade de conexões por agente do cluster

7.4.1.4.10.6. Load Average por servidor

7.4.1.4.10.7. Quantidade de espaço utilizado da quarentena

7.4.1.4.10.8. Quantidade de usuários

7.4.1.4.10.9. Data do ultimo update

7.4.1.4.10.10. Espaço de disco em uso

7.4.1.4.10.11. Swap

7.4.1.4.10.12. Percentual de utilização do cluster

7.4.1.4.11. Ter a capacidade de configurar single sign on (Autenticação de logon único) via SAML 2.0 com suporte as seguintes plataformas:

7.4.1.4.11.1. Microsoft AD FS 2.0 and 2.1
7.4.1.4.11.2. CA Single Sign-On (formerly CA Site Minder)
7.4.1.4.11.3. Ping Identity PingOne
7.4.1.4.11.4. Okta

7.4.1.4.12. Ter a capacidade de enviar uma mensagem de boas vindas automaticamente sempre que um novo usuário for criado e sincronizado no sistema ou criado manualmente, com informações sobre como acessar a quarentena e senha provisória.

7.4.1.4.13. Possuir cabeçalho de resposta HSTS (HTTP Secure Transport Security), ter incluído em todos os protocolos que suportam HTTPS sempre que o cliente tem instalado um certificado, o cabeçalho não será gerado se os certificados auto-assinados padrões estiverem sendo usados.

7.4.1.4.14. Das Funcionalidades para o Usuário Final:

7.4.1.4.14.1. Possuir interface web de administração segura HTTPS para que o usuário final possa administrar suas opções pessoais, sem que estas opções interfiram na filtragem dos demais usuários.
7.4.1.4.14.2. A interface do usuário final deve estar no idioma: “Português do Brasil”.
7.4.1.4.14.3. O usuário final deve ter a opção de escolher o perfil de filtragem de SPAM de acordo com perfis pré-configurados pelo administrador.
7.4.1.4.14.4. O usuário final deve ter a opção de escolher se quer ou não receber o resumo de e-mails bloqueados.
7.4.1.4.14.5. O usuário final deve poder incluir e remover endereços em sua lista pessoal de bloqueio ou de liberação de e-mails.
7.4.1.4.14.6. O usuário final deve poder visualizar as mensagens bloqueadas e libera-las, a seu critério.
7.4.1.4.14.7. O usuário final deve poder reportar ao administrador as mensagens indevidamente bloqueadas.

7.4.1.5. **Da Quarentena:**

7.4.1.5.1. Suportar a criação de áreas de quarentena personalizadas para grupos de usuários, bem como para usuários específicos.

7.4.1.5.2. A quarentena deve ser armazenada no próprio equipamento e, a escolha do administrador, deve ser armazenada criptografada.

7.4.1.5.3. O tempo de armazenamento da quarentena deve ser individual por área de quarentena, devendo também permitir armazenamento por tempo "indeterminado".

7.4.1.5.4. Excedido o tempo de vida estabelecido para a quarentena, as mensagens devem ser excluídas automaticamente.

7.4.1.5.5. Possibilitar a visualização do resumo de todas as áreas da quarentena, informando o tamanho de cada área, volume de mensagens e tempo de expiração.

7.4.1.5.6. Permitir ao administrador da solução executar pesquisa nas mensagens em quarentena de todos os usuários através de interface web segura (HTTPS), acessando o próprio equipamento, sem necessidade de nenhum software e hardware adicional.

7.4.1.5.7. Possibilitar o gerenciamento da quarentena pelo administrador, visualizando a razão do bloqueio, quem enviou, quem iria receber, a data, o assunto, o IP do host que enviou, a mensagem e seu tamanho, podendo liberar, excluir, mover ou processar novamente as mensagens.

7.4.1.5.8. Pelo sigilo da informação, permitir que determinadas áreas de quarentena somente sejam acessíveis a determinados administradores, permitindo a granularidade de acesso destas áreas.

7.4.1.6. **Dos Usuários e Grupos:**

7.4.1.6.1. Possuir integração com serviço de diretórios LDAP e Microsoft Active Directory, para obtenção de informações de usuários cadastrados para validação de destinatário e configuração de políticas.

7.4.1.6.2. Possuir a funcionalidade de filtrar individualmente, baseado em políticas definidas por domínio, subdomínio, grupo de usuários e usuário individual, de forma integrada com ferramentas de LDAP, mesmo que a mensagem seja destinada a múltiplos destinatários, em categorias distintas.

7.4.1.6.3. Permitir customizações de regras e políticas por usuários ou grupos.

7.4.1.7. **Dos Relatórios:**

7.4.1.7.1. Permitir a geração de relatórios de todos os equipamentos do cluster de forma centralizada e por interface única.
7.4.1.7.2. Gerar relatórios automatizados via agendamento, com envio dos mesmos para destinatários específicos, via SMTP.
7.4.1.7.3. Permitir seleção de dados para geração de relatórios por data específica ou intervalo de tempo, com granularidade de hora.
7.4.1.7.4. Possuir funcionalidade de configuração de período de retenção de dados para produção de relatórios.
7.4.1.7.5. Os relatórios devem ser disponibilizados em formato de gráfico, bem como em tabelas com dados dispostos em linhas e colunas.
7.4.1.7.6. Disponibilizar, pelo menos, os seguintes tipos de relatórios:
7.4.1.7.7. Sumário com total de mensagens classificadas como: spam, vírus, aceitas e com destinatários inválidos;
7.4.1.7.8. Sumário com os "n" maiores em envio de spam e vírus;
7.4.1.7.9. Relatórios sobre volume e tipo de spam recebido;
7.4.1.7.10. Relatórios de conexões SMTP: rejeitadas por reputação e rejeitadas por controle de conexões;
7.4.1.7.11. Possuir funcionalidade de exibição de gráficos com estatísticas no formato "*dashboard*" para acompanhamento em tempo real do fluxo de e-mails de cada um dos servidores de cluster com a possibilidade de customizar quais gráficos serão exibidos e sua posição na janela gráfica de maneira individual para cada administrador da ferramenta, contendo, no mínimo, as seguintes opções de gráficos *(wigets*):

7.4.1.7.11.1. Status dos servidores: memória, disco, processamento e sincronização;
7.4.1.7.11.2. Volume de mensagens;
7.4.1.7.11.3. Sumario de e-mails bloqueados;
7.4.1.7.11.4. Sumário de e-mails enviados e recebidos;
7.4.1.7.11.5. Sumário de e-mails enviados com criptografia;
7.4.1.7.11.6. Volume de conexões;
7.4.1.7.11.7. Estatísticas de vírus;
7.4.1.7.11.8. Estatísticas de spam;
7.4.1.7.11.9. Tamanho das mensagens;
7.4.1.7.11.10. Tempo das mensagens;

7.4.1.8. **Do Rastreamento das Mensagens:**

7.4.1.8.1. Permitir o rastreamento de mensagens, independente de qual equipamento do cluster processou, de forma centralizada e por meio da interface de gerenciamento HTTPS (não será aceito pesquisa via linha de comando).

7.4.1.8.2. O rastreamento deve ser possível através do: remente, destinatário, assunto da mensagem, nome do anexo, nome do vírus, regra de bloqueio e horário de entrega da mensagem.

7.4.1.8.3. O resultado do rastreamento deve informar: o remetente e destinatários da mensagem, o servidor de origem, se foi quarentenada, se continha vírus, a regra que atuou, o tamanho da mensagem e se foi entregue.

7.4.1.8.4. O rastreamento deve permitir a visualização da mensagem, caso tenha sido quarentenada.

7.4.1.8.5. O rastreamento deve apresentar o log com as evidências da entrega da mensagem, caso tenha sido entregue.

7.4.1.9. **Da Proteção Contra Ataques:**

7.4.1.9.1. Ser capaz de limitar o fluxo de mensagens automaticamente, de acordo com o volume de mensagens indevidas recebidas de um IP, fazendo a função de "*Rate Control*" com base em: volume de vírus, de spam e de remetentes inválidos, permitindo ao administrador configurar a sensibilidade de cada um dos gatilhos.

7.4.1.9.2. Ser capaz de controlar o número máximo de destinatários de um determinado emissor, por endereço IP, domínio, nome reverso, saudação SMTP ou país.

7.4.1.9.3. Permitir a inclusão de múltiplas listas de remetentes bloqueados em tempo real ("real-time black list-RBL"), permitindo regras de bloqueio se o IP estiver presente em "n" listas, configurável pelo administrador.

7.4.1.9.4. Possuir funcionalidade de verificação de SPF (*Sender Policy Framework*), permitindo regras individuais e customizadas para usuários ou grupos de usuários, permitindo criar ações específicas para "fail" e "soft fail", conforme descrito pelo Comitê Gestor da Internet no Brasil, no sítio: http://www.antispam.br/admin/spf

7.4.1.9.5. Prover a funcionalidade de rDNS (Reverse DNS *Lookup*).

7.4.1.9.6. Possuir controle de e-mail bounce (retorno de mensagem não enviada pelo usuário), passível de configuração pelo administrador.

7.4.1.9.7. Ter capacidade de bloquear conexões de e-mails nocivos antes do diálogo SMTP, permitindo a economia de banda, armazenagem e otimização do processamento, em especial baseado em lista local de bloqueio, RBLs e SPF.

7.4.1.10. **Da Proteção Contra SPAM:**

7.4.1.10.1. Possuir módulo de verificação com suporte a dois ou mais mecanismos diferentes de antispam, executando simultaneamente.

7.4.1.10.2. A análise de SPAM deve resultar a probabilidade heurística de a mensagem ser, no mínimo: SPAM, e-mail Marketing e e-mail Adulto.

7.4.1.10.3. A solução deve conter proteção específica para ataques do tipo "Phishing".

7.4.1.10.4. Permitir a aplicação de políticas de SPAM diferentes por Nome de Domínio do destinatário, Grupo de destinatários e por destinatário específico, integrando-se com AD/LDAP.

7.4.1.10.5. Suportar filtros de conexões providos pelo próprio fabricante, que deverão ser executados no início da conversação SMTP, com recomendações de, no mínimo: passar, rejeitar, tentar novamente e atrasar entrega.

7.4.1.10.6. Permitir filtros internos de "lista branca" e "lista negra" por endereços IP, Nome Reverso, bem como domínio e endereço, tanto de remetente, quanto de destinatário, permitindo o uso de expressões regulares.

7.4.1.10.7. Permitir regras internas para aumentar ou diminuir a probabilidade de ser SPAM com base em critérios internos, permitindo definir, no mínimo: idioma da mensagem, país de origem, endereço de domínio, IP e reverso do remente.

7.4.1.10.8. Detecta e classifica URLs maliciosos em e-mails . Este recurso, quando ativado como uma regra de política de spam, coloca em quarentena as mensagens que contenham URLs maliciosos em uma pasta de malware , em vez de uma pasta de spam. Isso garante que os usuários finais não possam inadvertidamente liberar e-mails com URLs maliciosas para sua caixa de entrada.

7.4.1.11. **Da Proteção Contra Vírus:**

7.4.1.11.1. Possuir módulo de verificação com suporte a dois ou mais mecanismos diferentes de antivírus, executando simultaneamente.

7.4.1.11.2. Possuir módulo de detecção "Hora Zero" para a identificação de novas ameaças desconhecidas pelo antivírus, colocando em determinada área da quarentena por período de tempo customizável, até nova verificação pelo antivírus.

7.4.1.11.3. Permitir regras específicas para surtos de vírus, como “I LOVE YOU”, com atuação distinta para o vírus especificado.

7.4.1.11.4. Tomar, no mínimo, as seguintes ações (simultaneamente): alterar o assunto da mensagem, adicionar cabeçalhos para rastreamento, descartar a mensagem, colocar em uma determinada área da quarentena definida pelo administrador, notificar o remetente e/ou destinatário com uma mensagem customizável, informando o nome do vírus.

7.4.1.12. **Da Gestão do MTA:**

7.4.1.12.1. Permitir a configuração de IPs virtuais, que permitirão a classificação de recebimento e envio por esses endereços.

7.4.1.12.2. Prover mecanismo que impeça a sua utilização como retransmissor de mensagens originadas externamente.

7.4.1.12.3. Tratar e analisar mensagens originadas e recebidas (*inbound* e *outbound*), possibilitando a aplicação de regras e políticas customizáveis, além de diferenciadas por sentido de tráfego.

7.4.1.12.4. Prover suporte ao envio e recebimento de mensagens utilizando protocolo TLS/SSL, permitindo configurar domínios onde TLS é mandatório.

7.4.1.12.5. Prover a assinatura das mensagens de saída com chave DKIM.

7.4.1.12.6. Fazer a análise de cabeçalho (header) nos padrões RFC 822.

7.4.1.12.7. Permitir a aplicação de regras baseadas no idioma que as mensagens foram escritas, com capacidade para, no mínimo, identificar Português, Inglês e Espanhol.

7.4.1.12.8. Controlar mensagens com base em dicionário de palavras com suporte a expressão regular e pontuação máxima por palavra, atuando de forma independente no conteúdo do anexo, do corpo do e-mail e do assunto.

7.4.1.12.9. Controlar conexões nos seguintes níveis, mediante configuração:

7.4.1.12.9.1. Número de mensagens por conexão;

7.4.1.12.9.2. Número de conexões simultâneas;

7.4.1.12.9.3. Número de destinatários por mensagem;

7.4.1.12.9.4. Tamanho das mensagens;

7.4.1.12.9.5. Tempo de processamento da mensagem;

7.4.1.12.10. Controlar mensagens com anexos com base em:

7.4.1.12.10.1. Mime Type;

7.4.1.12.10.2. Tipo real do arquivo;

7.4.1.12.10.3. Nome do arquivo;

7.4.1.12.10.4. Tamanho de anexo;

7.4.1.12.10.5. Quantidade de anexos;

7.4.1.12.10.6. Anexos compactados com senha;

7.4.1.12.10.7. Quantidade de camadas de arquivos compactados, um dentro do outro;

7.4.1.12.11. Todas as configurações do MTA devem ser granulares para domínios específicos e para grupos e usuários específicos;

7.4.1.12.12. Tomar, no mínimo, as seguintes ações: remover o anexo, alterar o assunto da mensagem, adicionar cabeçalhos para rastreamento, descartar a mensagem, colocar em uma determinada área da quarentena definida pelo administrador, notificar o remetente e/ou destinatário com uma mensagem customizável.

7.4.1.12.13. O MTA deve ser capaz de utilizar memória compartilhada, a configuração de memória compartilhada deve ser granular e configurável via interface gráfica.

7.4.1.12.14. Configurar tempo máximo de execução de um job de processamento de fila, permitindo configurar um intervalo menor para maior processamento de Jobs.

7.4.1.12.15. Quando uma única mensagem de e-mail é enviada para vários destinatários (aqueles em uma lista de discussão, por exemplo), um único processo MTA deve lidar com todos os destinatários. Caso esse processo morra, ou seja, derrubado no meio de processamento, não entregará a mensagem em partes. Como resultado, quando a fila é reprocessada mais tarde, os destinatários não receberão a mensagem duas vezes.

7.4.1.12.16. Ser capaz de configurar um limite total para todos os processadores de fila;

7.4.1.12.17. Ser capaz de definir o numero máximo de processadores de filas a serem executados em paralelo e em qualquer grupo de filas.

7.4.1.13. **Do Resumo de Bloqueio de Mensagens (Digest):**

7.4.1.13.1. O envio do Digest deve ocorrer em dias e horários estabelecidos pelo administrador.

7.4.1.13.2. Grupos diferentes de usuários devem poder receber o Digest em horários diferentes.

7.4.1.13.3. Grupos diferentes de usuários, bem como usuários específicos, devem poder configurar se receberão Digest vazio, na eventualidade de não existir mensagem bloqueada no período.

7.4.1.13.4. O Digest deve ser enviado em Língua Portuguesa e seu conteúdo deve poder ser customizado.

7.4.1.13.5. O Digest deve permitir ao usuário liberar a mensagem bloqueada e também reportar que o bloqueio é indevido.

7.4.1.14. **Da Atualização:**

7.4.1.14.1. Permitir a atualização automática das definições de vírus e SPAM, em intervalo de tempo configurado pelo administrador, permitindo atualizações de 5 em 5 minutos.

7.4.1.14.2. Permitir que se escolha, se os patches de segurança serão instalados automática ou manualmente.

7.4.1.14.3. Disponibilizar, durante a vigência da licença, o upgrade para a última versão estável do produto, sem custos adicionais.

7.4.1.14.4. Receber atualização automática de novos tipos de *Mime Type* na medida em que novos padrões são inventados e permitir inserção manual de tipos de Mype Type a serem definidas pelo Administrador.

7.4.1.15. **Da Expansão:**

7.4.1.15.1. A solução deverá suportar, para aquisição futura, a expansão, com implantação de módulo de DLP e Criptografia, para o número de usuários especificados, com as seguintes características:

7.4.1.15.1.1. Suportar a implantação de módulo de compliance na saída de e-mails para impedir, através de regras, a saída de informações sigilosas;

7.4.1.15.1.2. Suportar a implantação de módulo de compliance que permita consultar arquivos para aplicação de regras, impedindo o envio de determinado arquivo ou informação, mesmo que contida em arquivos dos tipos: .doc, .docx, .xls, xlsx, .pps, .ppsx, .pdf, .odf, .odt, .ods e .odp;

7.4.1.15.1.3. Suportar a implantação de módulo de *compliance* que permita aplicar tratamentos para mensagens que violarem regras de *compliance*, bloqueando, quarentenando e auditando a mensagem;

7.4.1.15.1.4. Suportar a implantação de módulo de *compliance* que possua a funcionalidade de cadastrar um determinado dicionário, a escolha

do administrador, bem como, possuir dicionários pré-configurados, na própria solução, para controles de regras de *compliance*;

7.4.1.15.1.5. Suportar a implantação de módulo de *compliance* que possibilite alteração de cabeçalho da mensagem, quando violada alguma regra de *compliance*;

7.4.1.15.1.6. Suportar a implantação de modulo de criptografia na saída de e-mails, que trabalhe de maneira transparente ao usuário, sem a necessidade de instalação de *plugins*, agentes ou outro tipo de software e possua interface para o destinatário customizável;

7.4.1.15.1.7. Suportar a implantação de módulo de criptografia com logs de auditoria de todas as transações envolvendo mensagens criptografadas;

7.4.1.15.1.8. Possuir console única de gerenciamento para interface de criptografia, *compliance*, *antispam* e antivírus, ou seja, para todos os módulos exigidos e suportáveis da solução;

7.4.1.15.1.9. Possibilitar ao administrador definir qual mensagem deverá ser criptografada, com base, no mínimo, em assunto, destinatário, remetente e anexo;

7.4.1.15.1.10. Possibilitar ao administrador integrar o DLP com a criptografia, de modo a que os e-mails sigilosos somente sejam enviados criptografados;

7.4.1.15.1.11. Utilização de criptografia das mensagens, geradas por chaves independentes;

7.4.1.15.1.12. Impossibilitar o uso de cache de browser para acesso as mensagens criptografadas;

7.4.1.15.1.13. O sistema deverá permitir que o modelo das mensagens criptografadas possa ser customizado;

7.4.1.15.1.14. O módulo já deve existir e conter todas as funcionalidades nativamente, bastando a expansão da licença, não sendo aceita a promessa de desenvolvimento até o momento da expansão.

7.4.1.16. **Características de Integração com a solução de Proteção de ameaças avançadas.**

7.4.1.16.1. A solução *AntiSpam* deve ser capaz de automaticamente enviar arquivos a serem analisados pela solução de proteção de ameaças avançadas ofertada.

7.5. CARACTERÍSTICAS MÍNIMAS DA SOLUÇÃO DE FILTRO WEB.

7.5.1. A solução deverá contemplar no mínimo **2 (dois)** appliances (Físicos ou Virtuais) com suporte a **3000 (três mil)** usuários licenciados;

7.5.2. A solução deverá suportar todos os protocolos de integração abaixo para maior facilidade de implementação na topologia da empresa:

7.5.2.1. ICAP;

7.5.2.2. HTTP;

7.5.2.3. HTTPS;

7.5.2.4. FTP;

7.5.2.5. WCCP;

7.5.3. A solução deverá suportar a todas modalidades de funcionamento abaixo descritas para implementação na topologia da empresa:

7.5.3.1. Proxy;

7.5.3.2. *Proxy* Reverso;

7.5.3.3. *Proxy* HA;

7.5.3.4. *Transparent Bridge*;

7.5.3.5. *Transparent Router*;

7.5.4. A solução deve ser capaz de suportar 300 Requisições/Segundo, sendo:

7.5.4.1. HTTP: responde por 60% das requisições;

7.5.4.2. HTTPS: responde por 40% das requisições;

7.5.5. Equipamento suporta configuração, manutenção e visualização de estado da solução através de CLI (Command Line Interface – Interface de Linha de Comando).

7.5.6. Equipamento deve suportar a montagem em Rack 19”.

7.5.7. A configuração das placas de rede da solução ofertada deve suportar tanto IPv4 como IPv6;

7.5.8. Em ambas configurações de IPv4 como IPv6 deve ser possivel a configuração do MTU;

7.5.9. A solução deve permitir a configuração manual e/ou automática de horário através de uso NTP configurada na solução.

7.5.10. O produto deve possuir proxy proprietários especificos para manuseio de todos protocolos abaixo citados:

7.5.10.1. HTTP

7.5.10.2. HTTPS

7.5.10.3. FTP

7.5.10.4. ICAP

7.5.10.5. IM Proxy

7.5.11. A configuração de ICAP deve permitir a configuração de todos os parametros abaixo citados:

7.5.11.1. Configuração da porta de funcionamento do proxy FTP.

7.5.11.2. Endereço IP responsável pelo manuseio das conexões FTP.

7.5.11.3. Configuração da porta de dados (DATA PORT).

7.5.11.4. Escopo de portas responsáveis por ouvir os clientes (*Port Range for client listener*).

7.5.11.5. Escopo de portas responsáveis por ouvir os servidores (*Port Range for server listener*).

7.5.11.6. Permitir ou não os clientes FTP a utilização de modo passivo de FTP;

7.5.12. A configuração de proxy FTP deve permitir a configuração de todos os parâmetros abaixo citados:

7.5.12.1. Configuração da porta de funcionamento ICAP;

7.5.12.2. Endereço IP responsável pelo manuseio das conexões ICAP;

7.5.12.3. Numero máximo de conexões concorrentes para REQMOD;

7.5.12.4. Numero máximo de conexões concorrentes para RESPMOD.

7.5.13. O produto deve possuir função de CACHE nativa na solução sem necessidades de produtos terceiros ou utilização de outros *appliances* para a realização desta função

7.5.14. Deve ser possível na configuração dos produtos um tempo de expiração de conexões para os protocolos HTTP(S), FTP e ICAP com os seguintes parâmetros:

7.5.14.1. Timeout para conexão inicial.

7.5.14.2. Timeout para conexões SERVER.

7.5.14.3. Timeout para conexões CLIENTS.

7.5.14.4. Timeout de conexão.

7.5.15. Este trafego SSL deve passar pelas mesmas políticas de filtragem aplicadas ao trafego não criptografado;

7.5.16. A Ferramenta deve possibilitar o uso de proxy streaming para os seguintes fins:

7.5.16.1. Redirecionamento de tráfego HTTP para HTTPS;

7.5.16.2. Prevenção de acesso a ferramentas de Open Proxy;

7.5.16.3. Balanceamento de carga;

7.5.16.4. *Caching;*

7.5.16.5. Criptografia SSL;

7.5.16.6. *Antimalware;*

7.5.17. A solução ofertada deve possuir filtro de reputação;

7.5.18. A solução ofertada deve possuir filtro de URL baseado em categorias, possuindo no mínimo mais de 90 categorias pré-definidas pelo fabricante;

7.5.19. A solução deve possuir solução *anti-malware* integrada ao *appliance*, ou seja, não serão aceitas soluções de *anti-malware* que necessitem de *appliances* adicionais para seu funcionamento.

7.5.20. O fabricante deste produto (solução ofertada) deve possuir laboratórios próprios para o desenvolvimento de vacinas/engines de antivirus, não sendo aceito uso de tecnologia OEM de terceiros para a realização desta função.

7.5.21. A solução ofertada deve suportar todas as versões abaixo para SNMP:

7.5.21.1. SNMP v1

7.5.21.2. SNMP v2c

7.5.21.3. SNMP v3

7.5.22. Características de Proxy da Solução

7.5.22.1. Suportar pelo menos os protocolos HTTP, HTTPS, FTP e IM.

7.5.22.2. Suportar active/passive mode FTP over HTTP.

7.5.22.3. Possuir a possibilidade de configuração das portas utilizadas para o serviço de Proxy.

7.5.22.4. Possuir a capacidade de utilizar o *proxy* com o método *CONNECT* para portas especificadas.

7.5.22.5. Permitir requisições dos clientes da rede interna em uma interface de rede e a comunicação com a Internet em outra interface, possibilitando usar um endereço IP privado na interface de rede interna e um IP público na interface de rede externa.

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

7.5.22.6.1. Endereço IP.
7.5.22.6.2. CIDR (Classless Inter-Domain Routing).
7.5.22.6.3. Domínio.
7.5.22.6.4. *Hostname* completo ou parte.

7.5.22.7. Possuir a capacidade de atuar como proxy explícito e transparente.

7.5.22.8. Atuar como proxy transparente através do redirecionamento de conexões utilizando WCCP.

7.5.22.9. Possuir integração com serviços de diretório LDAP e domínios Windows 2000 e 2003, 2008 para auditoria e autenticação sem a necessidade de instalação de agentes ou plugins em nenhuma estação de trabalho ou servidor.

7.5.22.10. A solução deverá ser capaz de criar e hospedar arquivos PAC (*Proxy Auto-configuration*).

7.5.22.11. Deverá suportar IP *Spoofing* para implementação em modo transparente.

7.5.22.12. A solução ofertada deve possuir serviço de *proxy* nativo e integrado ao *appliance* ofertada para gerenciamento de dados em tempo real, sem a necessidade de caixa adicionais para a realização deste serviço.

7.5.22.13. Produto deve possuir a capacidade de detecção automática de *Streaming*, com a finalidade de realizar *bypass* de *Antimalware* e controle de banda para esse tipo de tráfego.

7.5.23. FILTROS E CATEGORIAS DE URL E REPUTAÇÃO WEB

7.5.23.1. Atualizar a base de URLs, automaticamente via Internet, por meio de uma base proprietária do fornecedor que suporte os serviços e os *Appliances*;

7.5.23.2. Possuir uma base de URLs com no mínimo 90 (noventa) categorias pré-definidas e no mínimo 20 (vinte) milhões de domínios cadastrados;

7.5.23.3. Permitir a criação de no mínimo 500 (quinhentas) categorias extras customizadas (*user defined*);

7.5.23.4. A ferramenta deve ser capaz de realizar controle de banda para download/upload;

7.5.23.5. O Controle de Banda deve ser granular, ou seja, podendo ser aplicado com restrições aos seguintes parâmetros:

7.5.23.5.1. Grupo de usuários;
7.5.23.5.2. Horário;
7.5.23.5.3. Ip's;
7.5.23.5.4. Categoria do Site.

7.5.23.6. Possibilitar o envio ao fabricante da solução as URL´s não cadastradas na base de dados para análise e inclusão na base de categorias.

7.5.23.7. Possibilitar a criação de filtros URL's baseado em políticas de tempo, tais como dias da semana e range de horário, ou seja, alguns sites só poderão ser acessados fora do horário de expediente.

7.5.23.8. Deverá ser capaz de criar ações diferentes para as URL´s em políticas por tempo.

7.5.23.9. A ferramenta deve ser capaz de realizar a detecção de URLs frente a composição dos seguintes itens:

7.5.23.9.1. Url
7.5.23.9.2. Host
7.5.23.9.3. Domínio
7.5.23.9.4. Protocolo

7.5.23.9.5. Caminho da URL

7.5.23.10. Deverá permitir customização das páginas de notificações aos usuários.

7.5.23.11. A solução deverá detectar, monitorar e interceptar o acesso feito às páginas abertas dentro de servidores remotos, como:

7.5.23.11.1. Servidores de tradução.
7.5.23.11.2. Proxies anônimos.

7.5.23.12. As transações que forem detectadas deverão estar de acordo com as políticas estabelecidas pela empresa, onde o conteúdo não permitido que for acessado sob este mecanismo deverá ser bloqueado e o conteúdo dentro de políticas que permitem o acesso deverão ser acessados.

7.5.23.13. Possuir, no mínimo, as seguintes categorias URL:

7.5.23.13.1. Sites de conteúdos maliciosos.
7.5.23.13.2. Site de bate-papo (chat) e fóruns *on-ilne*.
7.5.23.13.3. Sites de *Anonymizers*
7.5.23.13.4. Sites com utilitários para *Anonymizing*.
7.5.23.13.5. Browser Exploits.
7.5.23.13.6. Sites de Encontros (*Dating*).
7.5.23.13.7. Sites de Discriminação.
7.5.23.13.8. Sites sobre Drogas.
7.5.23.13.9. Sites sobre Apostas.
7.5.23.13.10. Sites sobre conteúdo agressivo (*Gruesome Content*).
7.5.23.13.11. Site com downloads maliciosos.
7.5.23.13.12. Site com download de media.
7.5.23.13.13. Sites de compartilhamento de medias.
7.5.23.13.14. Instant Messaging.
7.5.23.13.15. P2P/File *Sharing*.
7.5.23.13.16. Sites para armazenamento de dados pessoais (*Personal Network Storage*).
7.5.23.13.17. Sites sobre Potenciais Atividades Criminais.
7.5.23.13.18. Sites sobre Potenciais Crimes de *Hacking*/Computer Crime.
7.5.23.13.19. Sites sobre Potenciais Softwares Ilegais.
7.5.23.13.20. PUPS

7.5.23.13.21. Endereços de IP Residencial
7.5.23.13.22. Shareware/Freeware
7.5.23.13.23. Spyware/Adware/Keyloggers
7.5.23.13.24. Web Mail

7.5.23.14. Possuir um sistema de filtro de reputação que permita estabelecer uma reputação para cada endereço IP dos servidores de destino, utilizando dados de uma rede mundial de monitoração de tráfego web e de e-mail para definir a reputação dos servidores de destino com cobertura global.
7.5.23.15. Permitir ações diferenciadas de acordo com cada reputação obtida, como bloquear, permitir ou verificar detalhadamente os objetos de cada acesso.

7.5.23.16. O produto deve ser capaz de realizar controle de aplicações web, aplicando políticas por aplicações específicas, usuários, grupos de risco de aplicação.

7.5.23.17. O Filtro de aplicação deve permitir configurar permissão de acesso de somente leitura para aplicações específicas.

7.5.23.18. Deve possuir capacidade de classificação de conteúdo dinâmico, aplicando auto-categorização aos websites que eventualmente estejam fora da lista local/nuvem.

7.5.24. Autenticação e Integração

7.5.24.1. A solução deverá permitir todos os métodos abaixo citados:

7.5.24.1.1. Autenticação do usuário via NTLM de modo transparente, ou seja, utilizando usuário já autenticado em domínio Windows sem pedir novamente a senha para o usuário;
7.5.24.1.2. Autenticação segura de clientes, ou seja, os dados de autenticação trocados entre o servidor de diretórios e o proxy criptografados, tanto para LDAP como para NTLM;
7.5.24.1.3. Autenticação baseada em LDAP;
7.5.24.1.4. Utilização de um NTLM-Agent, sendo um agente externo instalado em um sistema baseado em Windows para aplicação do método de autenticação NTLM;
7.5.24.1.5. Banco de dados de usuários em uma base na própria solução;
7.5.24.1.6. Através de servidores LDAP;

7.5.24.1.7. Através de servidores Novell eDirectory
7.5.24.1.8. Através de servidores RADIUS
7.5.24.1.9. Através de servidores Kerberos
7.5.24.1.10. Através de servidores de Autenticação Externo
7.5.24.1.11. Através do uso de cookies;
7.5.24.1.12. Básica (Basic Authentication) utilizando técnica de POPUP
7.5.24.1.13. NTLM over Proxy
7.5.24.1.14. Kerberos over HTTP

7.5.24.2. A solução ofertada deve possuir mecanismo de criação de regras a partir de lógica booleana permitindo flexibilidade e otimização a partir de parâmetros pré-definidos.

7.5.24.3. Autenticação (login, senha e domínio) para usuários que estejam utilizando sistemas operacionais diferentes do Windows (Linux, por exemplo), validando estes usuários no serviço de diretórios Microsoft Active Directory 2000/2003/2008.

7.5.24.4. Autenticação de usuários e estações de trabalho sem a necessidade de instalação e/ou execução de clientes ou quaisquer módulos em nenhuma estação de trabalho e/ou servidor.

7.5.24.5. Total integração com o Microsoft Active Directory 2000/2003 para autenticação de usuários e grupos, sem a necessidade de instalação e/ou execução de clientes ou quaisquer módulos nas estações de trabalho dos usuários ou nos servidores.

7.5.25. Criação de Regras, Conjunto de Regras e Listas

7.5.25.1. A solução deve permitir a criação dos conjuntos de regras e regras de forma ordem dependente.

7.5.25.2. A solução deve permitir a criação de conjunto de regras baseados em critérios para habilitação da mesma.

7.5.25.3. Estes critérios devem ser aplicados para Requisições, Respostas e Objetos incorporados de todas operações realizadas pelo produto ofertado.

7.5.25.4. O produto deve possuir pelo menos 400 propriedades para serem utilizadas pelas regras ou para os critérios de utilização das mesmas.

7.5.25.5. Aplicação do conjunto de regras devem se basear em todas as propriedades e permitindo a criação de lógica booleana entre estas propriedades e seus valores para decisão de habilitação ou não deste conjunto de regras.

7.5.25.6. Cada propriedade deverá ser testada através de operadores (igual, diferente, pertence a lista, não pertence a lista, maior que, maior que ou igual, menor que, ou menor que ou igual) para ser considerada válida ou não e com isso tomar a decisão se este conjunto de regras será testado ou não.

7.5.25.7. O produto deve possuir pelo menos as seguintes classes de propriedades abaixo citadas:

7.5.25.7.1. Antimalware
7.5.25.7.2. Probability
7.5.25.7.3. Authentication
7.5.25.7.4. BytestoClient
7.5.25.7.5. Block
7.5.25.7.6. Body
7.5.25.7.7. Cache
7.5.25.7.8. Category
7.5.25.7.9. Command
7.5.25.7.10. Client
7.5.25.7.11. Cache
7.5.25.7.12. DateTime
7.5.25.7.13. Error
7.5.25.7.14. HTML
7.5.25.7.15. Header
7.5.25.7.16. ICAP
7.5.25.7.17. IM
7.5.25.7.18. List
7.5.25.7.19. MediaType
7.5.25.7.20. PDStorage
7.5.25.7.21. ProgressPage
7.5.25.7.22. Proxy
7.5.25.7.23. Quota
7.5.25.7.24. Rules
7.5.25.7.25. Request
7.5.25.7.26. Response

7.5.25.7.27. SNMP
7.5.25.7.28. String
7.5.25.7.29. URL

7.5.25.8. Esta combinação de testes de propriedades deve permitir a validação das mesmas através de lógica definida pelo administrador da solução através de uso de operadores OR ou AND e permitir a combinação dos mesmos como exemplos abaixo:

7.5.25.8.1. a OR b OR c
7.5.25.8.2. (a OR b) AND c
7.5.25.8.3. (a AND b) OR c

7.5.25.9. Após validação desta regra o produto deve tomar as seguintes ações:

7.5.25.9.1. Autenticar
7.5.25.9.2. Bloquear
7.5.25.9.3. Continuar
7.5.25.9.4. Redirecionar
7.5.25.9.5. Remover
7.5.25.9.6. Parar analise do ciclo
7.5.25.9.7. Parar analise do conjunto de regras

7.5.25.10. A solução deve permitir o uso de listas nas regras utilizando a mesma lógica booleana abaixo explicada:

7.5.25.10.1. Categorias;
7.5.25.10.2. Autoridades Certificadoras;
7.5.25.10.3. Hosts e certificados confiáveis;
7.5.25.10.4. Endereços IPs;
7.5.25.10.5. Ranges IPs;
7.5.25.10.6. Usuários locais;
7.5.25.10.7. Tipo de mídia;
7.5.25.10.8. Números;
7.5.25.10.9. Strings;
7.5.25.10.10. Expressões Regulares (utilizando REGEX e/ou GLOB).

7.5.25.11. A solução deve possuir mecanismo de DLP nativo sem necessidade de licença adicional.

7.5.25.12. A solução deve ser capaz de integrar-se a ferramenta de DLP de Rede respondendo ao modo Request e Response

7.5.25.13. A ferramenta deve ser capaz bloquear o envio de documentos para Web baseado em extensão ou tipo de documento.

7.5.26. Anti-Malware e Antivirus

7.5.26.1. A solução deverá possuir módulo de antivírus, proprietária e de terceiros.

7.5.26.2. Pelo menos uma das *engines* de antivírus deve ser desenvolvida pelo próprio fabricante da solução ofertada.

7.5.26.3. A solução deve oferecer a opção de no mínimo dois mecanismos de antivírus rodando simultaneamente possibilitando uma camada adicional de filtragem;

7.5.26.4. Se houver algum atraso ou falha na realização da atualização automática, o equipamento deve ter a capacidade de alertar imediatamente o administrador através de logs, SNMP e E-mail.

7.5.26.5. Fazer analise de comportamento heurística das páginas que serão acessadas;

7.5.26.6. Identificar e bloquear aplicações Java Scripts maliciosas;

7.5.26.7. Identificar e bloquear aplicações Java applets maliciosas;

7.5.26.8. Identificar e bloquear aplicações Java applications maliciosas;

7.5.26.9. Identificar e bloquear aplicações ActiveX maliciosas;

7.5.26.10. Identificar e bloquear aplicações Flash ActionScripts

7.5.26.11. Identificar e bloquear aplicações executáveis Windows maliciosas;

7.5.26.12. Identificar e bloquear scripts Visual Basic maliciosos;

7.5.26.13. Identificar e bloquear aplicações Potencialmente Não Desejados (spywares, etc...);

7.5.26.14. Possuir tecnologia de analise em nuvem para arquivos suspeitos; esta tecnologia se baseia em enviar um *hash* do arquivo/código para o fabricante a fim do mesmo validar como uma aplicação maliciosa em tempo real e sem a necessidade de vacina instalada na solução ofertada.

7.5.26.15. Possuir filtros de análise de intenções para proteção pró-ativa contra ataques de dia zero com bloqueio de tráfego web em tempo real sem a necessidade de possuir uma assinatura;

7.5.26.16. A varredura deverá ser feita seqüencialmente no sistema, sem o uso de protocolos de comunicação entre as ferramentas como ICAP.

7.5.26.17. Detectar e bloquear "user agent" suspeitos.

7.5.26.18. A solução deve possibilitar bloquear todos os comportamentos/técnicas abaixo descritas:

7.5.26.18.1. Data theft: Backdoor
7.5.26.18.2. Data theft: Keylogger
7.5.26.18.3. Data theft: Password stealer
7.5.26.18.4. System compromise: Code execution exploit
7.5.26.18.5. System compromise: Browser exploit
7.5.26.18.6. System compromise: Trojan
7.5.26.18.7. Stealth activity: Rootkit
7.5.26.18.8. Viral Replication: Network worm
7.5.26.18.9. Viral Replication: File infector virus
7.5.26.18.10. System compromise: Trojan downloader
7.5.26.18.11. System compromise: Trojan dropper
7.5.26.18.12. System compromise: Trojan proxy
7.5.26.18.13. Web threats: Infected website
7.5.26.18.14. Stealth activity: Code injection
7.5.26.18.15. Detection evasion: Obfuscated code
7.5.26.18.16. Detection evasion: Packed code
7.5.26.18.17. Potentially unwanted: Ad-/Spyware
7.5.26.18.18. Potentially unwanted: Adware
7.5.26.18.19. Data theft: Spyware

7.5.26.18.20. Potentially unwanted: Dialer
7.5.26.18.21. Web threats: Vulnerable ActiveX controls
7.5.26.18.22. Potentially unwanted: Suspicious activity
7.5.26.18.23. Web threats: Cross-site scripting
7.5.26.18.24. Potentially unwanted: Deceptive behavior
7.5.26.18.25. Potentially unwanted: Redirector
7.5.26.18.26. Potentially unwanted: Direct kernel communication
7.5.26.18.27. Potentially unwanted: Privacy violation

7.5.27. Características de Gerenciamento da Solução

7.5.27.1. Possuir interface de gerência via Web e linha de comando na própria solução, ou seja, não serão aceitas soluções externas para o gerenciamento da solução de Proxy.

7.5.27.2. Possuir MIB própria para verificação das informações de utilização via SNMP.

7.5.27.3. Possibilitar o envio de alertas administrativos utilizando e-mails e *traps* SNMP.

7.5.27.4. Possibilitar a criação de políticas de acesso à interface de gerenciamento baseada em endereço IP e range de IP's que podem acessar o sistema.

7.5.27.5. Permitir a consulta da categoria de um determinado site através de servidor público na internet;

7.5.27.6. Deverá possuir pelo menos sete perfis de usuários de acesso:

7.5.27.6.1. Leitura e gravação
7.5.27.6.2. Somente Leitura
7.5.27.6.3. Sem permissão

7.5.27.7. A solução deverá permitir autenticação externa, para autenticar os usuários ao logar na gerência da solução através dos seguintes métodos de autenticação:

7.5.27.7.1. Através de servidores NTLM
7.5.27.7.2. Banco de dados de usuários em uma base na própria solução;
7.5.27.7.3. Através de servidores LDAP;
7.5.27.7.4. Através de servidores Novell e *Directory*.

7.5.27.7.5. Através de servidores RADIUS.

7.5.27.7.6. Através de servidores *Kerberos*.

7.5.28. Características de Integração com a solução de Gerência de *Endpoint*

7.5.28.1. Deve possuir agente gerenciado pela mesma console da gerência da solução *Endpoint*, que possua ao menos as seguintes capacidades:

7.5.28.1.1. Detectar e redirecionar a navegação ao *Proxy* de rede, garantindo assim que não seja necessária a reconfiguração dos navegadores das estações de trabalho.

7.5.28.1.2. Relatórios de navegação podem ser direcionadas a console de gerencia da solução *Endpoint* ofertada.

7.5.28.1.3. Possuir integração com a solução de Gestão de *Endpoint* para efetuar o controle dos sites acessados;

7.5.29. Relatórios

7.5.29.1. A solução deverá contemplar **1 (um)** servidor (Físico ou virtual) com a função exclusiva de gerenciamento de relatórios e logs;

7.5.29.2. A solução apresentada deverá possuir um mecanismo para geração de relatórios e logs;

7.5.29.3. Serão aceitos módulos de relatórios que rodem fora do *appliance* (out-of-box), desde que seja do mesmo fabricante.

7.5.29.4. Deve possuir ferramenta para análise de tráfego interativo, visando identificar o resultado das regras aplicadas, facilitando a metodologia de análise de problemas.

7.5.29.5. O módulo de relatório deverá se adequar aos padrões do Banpará, com suporte completo de instalação a todos os seguintes sistemas operacionais:

7.5.29.5.1. Windows 2008 Server

7.5.29.5.2. Windows 2012 Server

7.5.29.6. Deverá permitir a criação dos relatórios nos formatos HTML, PDF e CSV;

7.5.29.7. Deverá possuir no mínimo 30 relatórios pré-definidos, permitindo ao administrador configurar novos relatórios;

7.5.29.8. Permitir filtrar todos os relatórios com base em:

7.5.29.8.1. Sites
7.5.29.8.2. Nomes de usuários
7.5.29.8.3. Endereços IPs
7.5.29.8.4. Protocolo de Aplicação
7.5.29.8.5. Tipo de arquivos
7.5.29.8.6. Categorias
7.5.29.8.7. Malware
7.5.29.8.8. Reputação Web
7.5.29.8.9. Fonte de logs enviados (por appliance utilizado como fonte destes dados);

7.5.29.9. Permitir de forma opcional a criação de contas na ferramenta de relatório (*reporting account*) com restrição ao acesso a partes especifica dos dados com todos os filtros abaixo:

7.5.29.9.1. Usuários individuais ou grupos de usuários (usuários internos da ferramenta ou sincronizados com os de serviço de diretório como LDAP, AD, etc.)
7.5.29.9.2. Permitir atribuir colunas predefinidas, excluir colunas ou renomear colunas dos arquivos de log nos arquivos existentes. Isso deverá ser feito a partir de um assistente de customização de logs.

7.5.29.10. Deverá prover uma interface de monitoramento (Dashboard), monitorando a atividade de acesso web, incluindo:

7.5.29.10.1. Categorias;
7.5.29.10.2. Sites maliciosos – tentativas de acesso;
7.5.29.10.3. Sites acessados;

7.6. SOLUÇÃO DE PROTEÇÃO DAS ESTAÇÕES DE TRABALHO E SERVIDORES DE REDE

7.6.1. Características Básicas da Solução

7.6.1.1. A solução deverá contemplar no mínimo **2 (dois)** servidores (Físicos ou Virtuais) para gerenciamento da solução de proteção aos hosts;

7.6.1.2. Toda Solução de segurança proposta deverá ser fornecida por um único fabricante de modo que tanto o suporte a solução quanto as funcionalidades sejam inteiramente integradas e gerenciadas através de uma única console de gerenciamento.

7.6.1.3. Segurança para Servidores de Arquivos (Antivírus, *Antispyware*)

7.6.1.4. Suporte total aos sistemas operacionais baseados na plataforma *Windows*: Windows Server 2003 Standard, Windows Server 2003 Enterprise, Windows Server 2008 (Standard, Enterprise, Datacenter, Foundation, Web, HPC), Windows Small Business Server 2011, Windows Embedded Standard 2009 e Windows Server 2012.

7.6.1.5. Todas as funcionalidades deste item devem ser ativadas por agente único que facilita a instalação, a configuração e o gerenciamento.

7.6.1.6. Rastreamento em tempo real, para arquivos durante entrada e saída (gravação e leitura), com as seguintes opções: Limpar Arquivos Automaticamente, Excluir Arquivos Automaticamente e Negar Acesso aos Arquivos (quarentena).

7.6.1.7. Rastreamento manual com interface Windows, customizável, com opção de limpeza. Permitir diferentes configurações de varredura em tempo real baseando-se em processos de baixo ou alto risco, tornando assim o desempenho do produto mais estável.

7.6.1.8. Rastreamento em tempo real dos processos em memória, para a captura de vírus que são executados em memória sem a necessidade de escrita de arquivo. Detecção de programas maliciosos como spyware, programas de propaganda, ferramentas como *password crackers*, etc.

7.6.1.9. Programação de atualizações automáticas das listas de definições de vírus, a partir de local predefinido da rede, ou de site da Internet, com frequência (no mínimo diária) e horários definidos pelo administrador;

7.6.1.10. Permitir atualização incremental da lista de definições de vírus;

7.6.1.11. Salvar automaticamente as listas de definições de vírus em local especificado na rede, após cada atualização bem-sucedida.

7.6.1.12. Programação de rastreamentos automáticos do sistema com as seguintes opções:

7.6.1.12.1. Escopo: Todos os drives locais, drives específicos, ou pastas específicas;

7.6.1.12.2. Ação: Somente alertas, limpar automaticamente, apagar automaticamente, renomear automaticamente, ou mover automaticamente para área de segurança (quarentena);

7.6.1.12.3. Frequência: Horária, diária, semanal, mensal;

7.6.1.12.4. Exclusões: Pastas ou arquivos que não devem ser rastreados.

7.6.1.13. Gerar registro (log) dos eventos de vírus em arquivo e local definido pelo usuário, com limite de tamanho opcional;

7.6.1.14. Gerar notificações de eventos de vírus através de alerta na rede;

7.6.1.15. Permitir a instalação em ambientes em Cluster Microsoft;

7.6.1.16. Permitir bloqueio de aplicações pelo nome do arquivo;

7.6.1.17. Permitir bloqueio de portas;

7.6.1.18. Permitir criação de regras baseadas em processos de sistema;

7.6.1.19. Permitir o bloqueio de compartilhamentos da máquina em caso de epidemia;

7.6.1.20. Possuir proteção contra estouro de buffer;

7.6.1.21. Detecção de *cookies* potencialmente indesejáveis no sistema;

7.6.1.22. O sistema de *antispyware* deve estar totalmente integrado ao software antivírus utilizando a mesma biblioteca DAT de definições de vírus e demais ameaças;

7.6.1.23. O sistema deve estar integrado ao console de gerenciamento de segurança de sistemas, que também gerencia antivírus *antispyware*, IPS de Host e Firewall desktop. Possibilitando uma única e simples interface para gerenciar toda uma solução de segurança. Não deve ser instalado nenhum software adicional a console de gerenciamento para permitir o controle integrado.

7.6.1.24. Possuir proteção contra BOTs ;

7.6.1.25. Funcionar tanto no ambiente corporativo como em VPN;

7.6.1.26. Possuir instalação “silenciosa”;

7.6.1.27. Possuir gerenciamento centralizado;

7.6.1.28. Possibilitar a integração de políticas definidas pelo administrador com o usuário local;

7.6.1.29. Instalação automática em maquinas novas na rede, via software de gerencia;

7.6.2. Características para solução para estações de Trabalho 32 bits e 64 bits. (Antivírus, AntiSpyware, filtro web local, Controle de Dispositivos externos(USB) e IPS de Host)

7.6.2.1. Deve Suportar as plataformas Windows XP, Windows Vista, Windows 7, Windows 8 e Windows 10;

7.6.2.2. Suporte total a plataforma 64 bits.

7.6.2.3. Todas as funcionalidades deste item devem ser ativadas por agente único que facilita a instalação, a configuração e o gerenciamento.

7.6.2.4. Rastreamento em tempo real, para arquivos durante entrada e saída (gravação e leitura), com as seguintes opções: Limpar arquivos automaticamente; Excluir arquivos Automaticamente; Negar Acesso aos Arquivos (quarentena).

7.6.2.5. Rastreamento manual com interface Windows, customizável, com opção de limpeza.

7.6.2.6. Permitir diferentes configurações de varredura em tempo real baseando-se em processos de baixo ou alto risco, tornando assim o desempenho do produto mais estável.

7.6.2.7. Rastreamento em tempo real dos processos em memória, para a captura de vírus que são executados em memória sem a necessidade de escrita de arquivo.

7.6.2.8. Detecção de programas maliciosos como spyware, programas de propaganda, ferramentas como password crackers, etc...

7.6.2.9. Programação de atualizações automáticas das listas de definições de vírus, a partir de local predefinido da rede, ou de site da Internet, com Frequência (no mínimo diária) e horários definidos pelo administrador.

7.6.2.10. Permitir atualização incremental da lista de definições de vírus.

7.6.2.11. Salvar automaticamente as listas de definições de vírus em local especificado na rede, após cada atualização bem-sucedida.

7.6.2.12. Programação de rastreamentos automáticos do sistema com as seguintes opções:

7.6.2.12.1. Escopo: Todos os drives locais, drives específicos, ou pastas específicas;

7.6.2.12.2. Ação: Somente alertas, limpar automaticamente, apagar automaticamente, renomear automaticamente, ou mover automaticamente para área de segurança (quarentena);

7.6.2.12.3. Frequência: Horária, diária, semanal, mensal;

7.6.2.12.4. Exclusões: Pastas ou arquivos que não devem ser rastreados.

7.6.2.13. Gerar registro (log) dos eventos de vírus em arquivo e local definido pelo usuário, com limite de tamanho opcional.

7.6.2.14. Gerar notificações de eventos de vírus através de alerta na rede.

7.6.2.15. Permitir a instalação em ambientes em Cluster Microsoft.

7.6.2.16. Permitir bloqueio de aplicações pelo nome do arquivo.

7.6.2.17. Permitir o bloqueio do compartilhamento caso uma ameaça seja detectada em uma pasta compartilhada.

7.6.2.18. Permitir o bloqueio de compartilhamentos da máquina em caso de epidemia.

7.6.2.19. Possuir proteção contra estouro de *buffer*.

7.6.2.20. Detecção de *cookies* potencialmente indesejáveis no sistema.

7.6.2.21. O sistema de *antispyware* deve estar totalmente integrado ao *software* antivírus utilizando a mesma biblioteca DAT de definições de vírus e demais ameaças.

7.6.2.22. O sistema deve estar integrado ao console de gerenciamento de segurança de sistemas, que também gerencia antivírus antispyware, IPS de Host e Firewall desktop. Possibilitando uma única e simples interface para gerenciar toda uma solução de segurança. Não deve ser instalado nenhum software adicional a console de gerenciamento para permitir o controle integrado.

7.6.2.23. Oferecer proteção avançada de sistemas contra ameaças tais como ataques remotos de injeção de SQL ou HTTP.

7.6.2.24. Deve possuir o recurso de blindagem, impedindo o comprometimento dos aplicativos e dos seus dados, além de evitar que um aplicativo seja usado para atacar outros aplicativos.

7.6.2.25. Possuir proteção completa, pronta para operação e contra vulnerabilidades desconhecidas, tais como estouro de buffer (buffer overflow) e ataques de dia zero (zero-day attacks).

7.6.2.26. Possuir proteção contra BOTs.

7.6.2.27. Capacidade de trabalhar no modo adaptativo se adaptando a novas aplicações instaladas na máquina.

7.6.2.28. Disponibilizar os seguintes relatórios na plataforma de gerência: sumário de eventos de IPS por assinatura, por alvo, por endereço IP origem, os 10 principais nós atacados, as 10 principais assinaturas, sumário das aplicações bloqueadas e *update* de quarentena.

7.6.2.29. Permitir o bloqueio de ataques baseados em Web como: *Directory Traversal Attacks* e *Unicode Attacks*.

7.6.2.30. Interceptar tráfego e requisições de HTTP após decriptação e decodificação.

7.6.2.31. Prevenir o roubo de informações de um servidor Web, ou mesmo que um hacker com privilégios de *root* possa manipular o servidor Web.

7.6.2.32. Permitir criação de política que somente permita tráfego de rede de saída da máquina depois que o cliente de IPS de *Host* estiver sendo executado.

7.6.2.33. Permitir o bloqueio de aplicações e os processos que a aplicação interage.

7.6.2.34. Capacidade de detectar e bloquear tentativas de invasão.

7.6.2.35. Possuir instalação “silenciosa”.

7.6.2.36. Possuir gerenciamento centralizado.

7.6.2.37. Bloquear acessos indevidos que não estejam na tabela de políticas definidas pelo administrador.

7.6.2.38. Permitir monitoração de aplicações onde pode-se determinar quais processos poderá ou não ser executados.

7.6.2.39. Permitir monitoração de *Hooking* de aplicações onde se podem determinar quais processos pode ou não ser executado.

7.6.2.40. Permitir criar regras de bloqueio/permissão utilizando protocolos ou aplicações.

7.6.2.41. Permitir configuração de regras por horários.

7.6.2.42. Possuir integração com a mesma ferramenta de gerencia do antivírus.

7.6.2.43. Possibilitar a integração de políticas definidas pelo administrador com o usuário local.

7.6.2.44. Instalação automática em maquinas novas na rede, via software de gerencia.

7.6.2.45. Possuir ferramenta para verificação de reputação de *websites*.

7.6.2.46. Possibilidade de configuração de bloqueio de acesso aos sites maliciosos pela console de gerenciamento.

7.6.2.47. Possibilidade de criar *blacklists* e *whitelists* de Urls para estações pela console de gerenciamento.

7.6.2.48. Possuir módulo de proteção de navegação a determinado conteúdo na internet possuindo pelo menos 80 categorias de *websites*.

7.6.2.49. Esta categorização deve ser atualizada constantemente e automaticamente pelo fabricante a fim de prover maior qualidade deste serviço.

7.6.2.50. Possuir pelo menos as categorias: Sites de Armas, de material adulto, de drogas, de educação, de entretenimento, de jogos,de governo, de saúde, de Tecnologia da Informação, Comunicação na Internet, pesquisa de emprego, notícias e mídia, de religião, de compras, de viagens, violências, Sites de rádio e tv pela internet, telefonia pela internet e streaming de media, Sites de compartilhamento de arquivos ponto-a-ponto (P2P), Sites de downloads de freeware ou software, de mensagens instantâneas, de *phising*, *keyloggers*, redes de *bots*, *websites* maliciosos, softwares potencialmente indesejados e spyware e Sites de conteúdo potencialmente perigoso, exposição elevada e explorações emergentes.

7.6.2.51. A solução deve ser capaz de identificar sistemas gerenciados ou não pela console de gerenciamento.

7.6.2.52. A solução devera controlar dispositivos removíveis permitindo o gerenciamento dos mesmos pela mesma console de administração de toda solução.

7.6.2.53. Controlar o modo como os usuários copiam dados em *drives* USB, iPods, CDs regraváveis e DVDs, disquetes, dispositivos *Bluetooth* e IrDA, dispositivos de leitura de imagens, portas COM e LPT e outros.

7.6.2.54. Especificar quais dispositivos podem ou não ser usados por qualquer parâmetro de dispositivo, inclusive códigos de produtos, códigos de fornecedor, números de série, classes de dispositivos, nomes de dispositivos.

7.6.2.55. Coletar dados de incidentes tais como dispositivo, data/hora, evidências de dados e outros, para reação, investigação e auditoria.

7.6.2.56. Permitir regra de reação para unidades de mídia removível (ex.: *pen-drive*) com as opções de bloqueio total, somente leitura e monitoramento.

7.6.2.57. Monitorar automaticamente o uso e bloquear todas as tentativas de uso dos dispositivos ou transferência de dados contrários às políticas definidas.

7.6.2.58. Integração com estrutura de *Active Directory* para criação de regras baseadas em usuários ou grupos de usuários.

7.6.3. Solução para Gerenciamento de ativos, integrado ao processador da máquina

7.6.3.1. Deve suportar os seguintes sistemas operacionais: Windows XP SP3, Windows 7, Windows 8, Windows 10, Windows 2003, Windows 2008 e Windows Server 2012.

7.6.3.2. A solução deve ser gerenciada pela mesma console de gerenciamento de toda a solução Endpoint.

7.6.3.3. A solução deve integrar-se a arquitetura a partir da segunda geração dos processadores Intel vPRO i5 e i7.

7.6.3.4. Deve permitir operação por trás do sistema operacional, habilitando ações baseadas no processador mesmo sem o carregamento total do sistema operacional.

7.6.3.5. Executar inventário de hardware dos desktops, mostrando quais máquinas estão aptas a receber o produto, baseado em sua versão de processador e vPRO(AMT).

7.6.3.6. Possibilidade de ligar os desktops remotamente a partir de tecnologia presente nos processadores.

7.6.3.7. Após ligar os *desktops*, em conjunto com as tarefas da solução de endpoint, deve ser possível varrer a máquina em busca de novas ameaças ou mesmo atualizar as definições de vírus, para em seguida desligar o terminal.

7.6.3.8. Deve ser possível agendar uma tarefa para ligar as máquinas remotamente em determinado horário pré estabelecido.

7.6.3.9. Deve possuir funcionalidade para IDE *Redirection* que consiste em remotamente iniciar o terminal com um boot de uma mídia alternativa, possibilitando assim carga remota de novas imagens .iso.

7.6.3.10. Deve permitir controle de Teclado, Video e Mouse remotamente utilizando a função KVM dos processadores Intel vPro.

7.6.3.11. A solução deve entregar ao menos os seguintes tipos de relatórios:

7.6.3.11.1. Sistemas capazes de receber a instalação da solução;

7.6.3.11.2. Sistemas que não tem uma CPU compatível com a solução;

7.6.3.11.3. Eventos recebidos.

7.6.4. Solução de Segurança para Ambientes Virtualizados.

7.6.4.1. Arquitetura de Solução:

7.6.4.1.1. Deve ser uma solução antivírus que remove a necessidade da instalação de agentes de varredura em todas as máquinas virtuais hospedadas em um servidor de virtualização.

7.6.4.1.2. A solução deve implementar o uso de um servidor de varredura *Offload*, que será responsável por escanear todos os acessos de arquivos nas máquinas virtuais hospedadas em determinado servidor *Hypervisor*, resultando assim em menos consumo de recursos e melhoria de performance.

7.6.4.1.3. A solução deve prover gerenciamento centralizado, a partir da mesma solução de gerência já utilizada pelos agentes de antivirus convencionais utilizados na rede (ePO - Eletronic Policy Orchestrator).

7.6.4.1.4. Esse servidor de gerenciamento deve servir também como repositório de políticas e atualizações para o produto de proteção a virtualização.

7.6.4.1.5. O servidor de varredura *offload* deve permitir a implementação em alta disponibilidade, aumentando assim o nível de segurança e deixando o ambiente preparado para o evento de falha do servidor de varredura.

7.6.4.1.6. O módulo para proteção de infra-estrutura virtual, deverá proporcionar, no mínimo, a proteção de ambientes virtualização VMWare e Citrix.

7.6.4.1.7. A solução deverá permitir a sua implantação atendendo no mínimo uma das seguintes opções:

7.6.4.1.7.1. Multi-Plataforma, atuando para realizar o rastreamento em tempo real, por demanda e agendado de *malwares*, através da utilização de uma máquina virtual com a solução Antivírus instalada efetuando todas as análises da estrutura, sem a necessidade de qualquer integração com agentes externos ou a instalação de clientes Antivírus em cada uma das máquinas virtuais;

7.6.4.1.7.2. *Agentless* (sem agente), atuando para realizar o rastreamento em tempo real, por demanda e agendado de *malwares*, através de integração com o VMWare vShield 5.0 ou superior utilizando o

VMWare vShield para rastreamento automático em ambientes que contem o SVA (*Storage Virtual Appliance*).

7.6.4.2. Sistemas Operacionais Suportados para o servidor de varredura Offload:

7.6.4.2.1. Windows 2008 R2 SP1
7.6.4.2.2. Windows 2008 SP2 (64-bit)

7.6.4.3. Sistemas Operacionais Suportados nas máquinas virtuais a serem varridas em busca de ameaças:

7.6.4.3.1. Windows XP SP3
7.6.4.3.2. Windows 7 (32 ou 64 bits)
7.6.4.3.3. Windows 8 (32 ou 64 bits)
7.6.4.3.4. Windows 2003 R2 SP2 (32-bits)
7.6.4.3.5. Windows 2008 SP2 (32 ou 64 bits)
7.6.4.3.6. Windows 2008 R2 SP1 (64 bits)
7.6.4.3.7. Windows Vista (32 ou 64 bits)
7.6.4.3.8. Windows 10 (34 ou 64 bits)
7.6.4.3.9. Windows Server 2012)

7.6.4.4. Console de Gerência da Solução:

7.6.4.4.1. Suporte a instalação em um servidor nas plataformas Windows Server 2003 (Com Service Pack 2 ou Superior) 32 e 64 bits, Windows Server 2008 (Com Service Pack 2 ou superior) 32 e 64 bits e Windows 2008 Server R2 e Windows 2008 Small Business Server somente em 64-bit e Windows Server 2012;
7.6.4.4.2. O Gerenciador pode trabalhar em modo Cluster;
7.6.4.4.3. O gerenciador provê ferramentas de Backup e Restore;
7.6.4.4.4. A ferramenta de gerência deve possibilitar autenticação externa integrada a estrutura LDAP;
7.6.4.4.5. A ferramenta de gerência deve suportar o gerenciamento de políticas de senha de autenticação na console;
7.6.4.4.6. A solução de gerenciamento deve permitir acesso a sua console via web;

7.6.4.4.7. Implementação de Dashboard com medição do nível de atualização do ambiente e o nível de cumprimento de política de segurança previamente definida;

7.6.4.4.8. Permitir a alteração das configurações Módulos da Solução nos clientes de maneira remota;

7.6.4.4.9. Permitir a distribuição remota do agente de proteção para as máquinas virtuais;

7.6.4.4.10. Permitir a distribuição remota do software para os servidores que hospedam as máquinas virtuais;

7.6.4.4.11. Permitir o gerenciamento do servidor através do protocolo TCP/IP e HTTP;

7.6.4.4.12. A ferramenta de gerência deve suportar a autenticação com segregação de funções, possibilitando a criação de usuários com diferentes níveis de permissão (Relatórios, auditoria, configuração);

7.6.4.4.13. Customização dos relatórios gráficos gerados;

7.6.4.4.14. Exportação dos relatórios para formatos HTML, CSV e PDF.

7.6.4.4.15. Geração de relatórios que contenham as seguintes informações:

7.6.4.4.15.1. Os vírus que mais foram detectados;

7.6.4.4.15.2. As máquinas que mais sofreram infecções em um determinado período de tempo;

7.6.4.4.15.3. Os usuários que mais sofreram infecções em um determinado período de tempo.

7.6.4.4.16. Gerenciamento de todos os módulos da suíte;

7.6.4.4.17. Deve possuir log de auditoria, logando todas as ações dos usuários na console de gerenciamento.

7.6.4.5. Políticas/ Configuração

7.6.4.5.1. A aplicação deve conter um conjunto de políticas pré-configuradas;

7.6.4.5.2. A solução deverá permitir a realização de varreduras por demandas em máquinas virtuais que estiverem em estado "offline';

7.6.4.5.3. O servidor de varredura *offload* deve permitir acesso à configuração e verificação de estatísticas via linha de comando CLI (*Command Line Interface*);

7.6.4.5.4. Deverá permitir a tomada de no mínimo as seguintes ações quando uma ameaça for identificada no servidor ou nas máquinas clientes:

7.6.4.5.4.1. Limpar o arquivo automaticamente;

7.6.4.5.4.2. Excluir o arquivo automaticamente;

7.6.4.5.4.3. Negar o acesso ao arquivo;

7.6.4.5.4.4. Na falha da execução da primeira ação deverá permitir a configuração de ação secundária com no mínimo as seguintes opções:

7.6.4.5.4.5. Excluir o arquivo automaticamente;

7.6.4.5.4.6. Negar o acesso ao arquivo;

7.6.4.5.4.7. Deverá permitir a aplicação de ações diferenciadas para *Malwares* e programas potencialmente indesejados (PUP´s);

7.6.5. Módulo para Gerenciamento da Solução – gerência centralizada de todos os módulos da suíte:

7.6.5.1. Suporte a instalação em um servidor nas plataformas Windows Server 2003 (Com Service Pack 2 ou Superior) 32 e 64 bits, Windows Server 2008 (Com Service Pack 2 ou superior) 32 e 64 bits, Windows 2008 Server R2, Windows 2012 Server, Windows 2012 Server R2.

7.6.5.2. Suporte a instalação em cluster Microsoft.

7.6.5.3. Permitir o gerenciamento do servidor através do protocolo TCP/IP e HTTP.

7.6.5.4. Permitir a instalação dos Módulos da Solução a partir de um único servidor.

7.6.5.5. Permitir a alteração das configurações Módulos da Solução nos clientes de maneira remota.

7.6.5.6. Possuir a integração com o gerenciamento da solução de segurança de estações de trabalho e servidores, deste mesmo fabricante a fim de prover uma única console de gerenciamento centralizado de todas as soluções de segurança que possam ser utilizadas pela CONTRATANTE na contratação presente ou em futuras.

7.6.5.7. Permitir a atualização incremental da lista de definições de vírus nos clientes, a partir de um único ponto da rede local.

7.6.5.8. Visualização das características básicas de hardware das máquinas.

7.6.5.9. Integração e Importação automática da estrutura de domínios do *Active Directory* já existentes na rede local.

7.6.5.10. Permitir a criação de tarefas de atualização, verificação de vírus e upgrades em períodos de tempo pré-determinados, na inicialização do Sistema Operacional ou no Logon na rede.

7.6.5.11. Permitir o armazenamento das informações coletadas nos clientes em um banco de dados centralizado.

7.6.5.12. Permitir diferentes níveis de administração do servidor, de maneira independente do login da rede.

7.6.5.13. Suporte a múltiplos usuários, com diferentes níveis de acesso e permissões aos produtos gerenciados.

7.6.5.14. Criação de grupos de máquinas baseadas em regras definidas em função do número IP do cliente.

7.6.5.15. Permitir a criação de grupos virtuais através de "TAGs".

7.6.5.16. Permitir aplicar as "TAGs" nos sistemas por vários critérios, incluindo: produtos instalados, versão de sistema operacional, quantidade de memória, etc...

7.6.5.17. Forçar a configuração determinada no servidor para os clientes;

7.6.5.18. Caso o cliente altere a configuração, a mesma deverá retornar ao padrão estabelecido no servidor, quando a mesma for verificada pelo agente.

7.6.5.19. A comunicação entre as máquinas clientes e o servidor de gerenciamento deve ser segura usando protocolo de autenticação HTTPS.

7.6.5.20. Forçar a instalação dos Módulos da Solução nos clientes;

7.6.5.21. Caso o cliente desinstale os Módulos da Solução, os mesmos deverão ser reinstalados, quando o agente verificar o ocorrido.

7.6.5.22. Características quanto à Customização dos relatórios e gráficos gerados;

7.6.5.23. Exportação dos relatórios para formatos HTML, CSV, PDF, XML;

7.6.5.24. Geração de relatórios que contenham as seguintes informações:

7.6.5.24.1. Máquinas com a lista de definições de vírus desatualizada;
7.6.5.24.2. Qual a versão do software (inclusive versão gerenciada pela nuvem) instalado em cada máquina;
7.6.5.24.3. Os vírus que mais foram detectados;
7.6.5.24.4. As máquinas que mais sofreram infecções em um determinado período de tempo;
7.6.5.24.5. Os usuários que mais sofreram infecções em um determinado período de tempo;

7.6.5.25. Gerenciamento de todos os módulos da suíte;

7.6.5.26. Possuir *dashboards* no gerenciamento da solução:

7.6.5.26.1. Estes *dashboards* devem conter, no mínimo, os seguintes relatórios de fácil visualização:

7.6.5.26.1.1. Cobertura da proteção de Navegação Segura;
7.6.5.26.1.2. Relatório dos últimos 30 dias da detecção de códigos maliciosos;
7.6.5.26.1.3. Top 10 Computadores com Infecções;
7.6.5.26.1.4. Top 10 Computadores com Sites bloqueados pela política;
7.6.5.26.1.5. Resumo das ações tomadas nos últimos 30 dias no que se refere a Filtro de Navegação na web;
7.6.5.26.1.6. Resumo dos tipos de sites acessados nos últimos 30 dias no que se refere a Filtro de Navegação Segura;

7.6.5.27. Gerenciar a atualização do antivírus em computadores portáteis (notebooks), automaticamente, mediante conexão em rede local ou remota.

7.6.5.28. Suportar o uso de múltiplos repositórios para atualização de produtos e arquivo de vacina com replicação seletiva.

7.6.5.29. Ter a capacidade de gerar registros/logs para auditoria.

7.6.5.30. A solução de gerenciamento deve ter a capacidade de atribuir etiquetas às máquinas, facilitando assim a distribuição automática dentro dos grupos hierárquicos na estrutura de gerenciamento.

7.6.5.31. A solução de gerenciamento deve permitir acesso a sua console via web.

7.6.5.32. Implementação de *Dashboard* com medição do nível de atualização do ambiente e o nível de cumprimento de política de segurança previamente definida.

7.6.6. Solução de Lista Branca (White List) para desktops

7.6.6.1. A solução deve suportar as seguintes modalidades de proteção:

7.6.6.1.1. *Application Whitelisting*: criação de uma lista de aplicações autorizadas que podem ser executadas no equipamento, onde todas as demais aplicações são impedidas de serem executadas;

7.6.6.1.2. *Application Blocking / Blacklisting*: criação de uma lista de aplicações não autorizadas que não podem ser executadas;

7.6.6.1.3. *Memory Protection*: monitoração e proteção de aplicativos e componentes críticos do sistema operacional de serem adulterados em tempo de execução, isto é, durante operação e execução em memória;

7.6.6.1.4. *Change Control*: Deve monitorar mudanças de arquivos e chaves de registro em tempo real;

7.6.6.2. Sistemas Operacionais suportados para as estações/servidores com a solução instalada: Microsoft Windows XP SP3, Microsoft Windows 7 (32 ou 64 bits), Microsoft Windows Vista (32 ou 64 bits), Microsoft Windows NT 32 bit, Microsoft Windows 2000 32 bit, Microsoft Windows 8 (32 ou 64 bits), Microsoft Windows 10 (32 ou 64 bits) e Microsoft Windows Server 2012.

7.6.6.3. Exportação dos relatórios para os formatos HTML, CSV, PDF e XML.

7.6.6.4. Geração de relatórios que contenham as seguintes informações:

7.6.6.4.1. Eventos detectados em tempo real;

7.6.6.4.2. Usuários que mais tentaram a modificação de arquivos monitorados

7.6.6.4.3. Histórico de eventos, e configurável por datas.

7.6.6.5. Deve possuir log de auditoria, ligando todas as ações dos usuários na console de gerenciamento.

7.6.6.6. A aplicação deve conter um conjunto de políticas pré-configuradas.

7.6.6.7. A solução deverá permitir a realização de varreduras por demandas em máquinas para executar a blindagem de aplicativos.

7.6.6.8. Solução suporta criação, configuração e manutenção de políticas através de CLI (*Command Line Interface*) no caso de falha de conexão com a gerência centralizada.

7.6.6.9. Solução suporta as modalidades de operação *Online* ou *Offline*.

7.6.6.10. Solução suporta algoritmo de verificação de aplicações – algoritmo de verificação SHA-1 (*Secure Hash Algorithm*).

7.6.6.11. Solução suporta operação com impacto mínimo nos ciclos de CPU (*Central Processing Unit*) e consumo de memória abaixo de 10 MB (Megabytes).

7.6.6.12. Solução deve suportar criação, configuração e manutenção de *Whitelist* dinamicamente através de definição de regras de confiança.

7.6.6.13. A solução deve suportar os seguintes mecanismos:

7.6.6.13.1. Application Code Protection: permite que somente os programas em Whitelist (executáveis, binários, DLLs, Scripts, extensões customizadas, etc) possam ser executados. Além disso, permite proteção contra adulterações de programas em *Whitelist* (ex.: arquivos do programa) e, opcionalmente, chaves de registros contra modificações em disco.

7.6.6.13.2. *Memory Protection*: permite proteção contra ataques e exploração de vulnerabilidades para os programas em *Whitelist*.

7.6.6.14. Suporte a criação, configuração e manutenção de políticas, permitindo ou bloqueando a adesão de *Whitelist*, através de:

7.6.6.14.1. *Binary*: binário específico identificado através de seu nome ou de algoritmo de verificação SHA-1.

7.6.6.14.2. *Trusted Publisher*: fornecedor específico, assinado digitalmente por um certificado de segurança emitido, para este fornecedor, por uma Autoridade Certificadora (CA – *Certificate Authority*).

7.6.6.14.3. *Trusted Installer*: software instalado por um programa instalador específico, identificações por seu algoritmo de verificação, independentemente de sua origem.

7.6.6.14.4. *Trusted Directories*: pasta compartilhada na rede, onde os programas instaladores para aplicações autorizadas e licenciadas são mantidos.

7.6.6.14.5. *Trusted Program / Authorized Updater*: programas identificados pelo nome, para adicionar e/ou atualizar aplicações.

7.6.6.14.6. *Trusted Users / Authorized Users*: somente usuários selecionados, substituindo a proteção de adulteração, para adicionar e/ou atualizar aplicações.

7.6.6.14.7. *Trusted Time Window / Update Mode*: janela de tempo para manutenção de aplicações.

7.6.7. Antivírus para Servidores de Groupware

7.6.7.1. Servidores Microsoft Exchange Server:

7.6.7.1.1. Compatíveis com as plataformas Windows 2003, Windows 2008 e Windows 2012.

7.6.7.1.2. Suporte a *Exchang*e 2007 SP2 ou superior, *Exchange* 2010 SP2 ou superior e *Exchange* 2013.

7.6.7.1.3. Rastreamento em tempo real, para arquivos anexados a mensagens do *Exchange*, antes de entregá-la a caixa postal do(s) destinatário(s), com as seguintes opções:

7.6.7.1.3.1. Limpar o arquivo infectado e entregá-lo limpo para o(s) destinatário(s);

7.6.7.1.3.2. Gravar o arquivo infectado na área de segurança (quarentena) e não entregá-lo para o(s) destinatário(s);

7.6.7.1.3.3. Gerar notificações e alertas e entregar o arquivo para o(s) destinatário(s);

7.6.7.1.3.4. Rastreamento manual as pastas do Exchange, com opção de limpeza.

7.6.7.1.4. Programação de rastreamentos automáticos do Exchange com as seguintes opções:

7.6.7.1.4.1 Escopo: Todas as pastas locais, ou pastas específicas;

7.6.7.1.4.2 Ação: Somente alertas, limpar, apagar, renomear ou mover, tudo automaticamente, para a área de segurança (Quarentena);

7.6.7.1.4.3 Frequência: Horária, diária, semanal e mensal.

7.6.7.1.5. Gerar registro (log) dos eventos de vírus em arquivo e local definido pelo usuário, com limite de tamanho opcional;

7.6.7.1.6. Gerar notificações de eventos de vírus através de mensagens do Exchange para quem enviou e quem recebeu a mensagem, e para um Administrador (usuário opcional);

7.6.7.1.7. Identificação de remetente e destinatário das mensagens

7.6.7.1.8. Permitir bloqueios baseados nos seguintes critérios: Tipo de arquivo, nome do arquivo e tamanho do arquivo.

7.6.7.1.9. Permitir a instalação em ambientes em Cluster Microsoft;

7.6.7.1.10. Capacidade de filtragem de conteúdo por categorias como: Sexo, Drogas, etc...

7.7. SOLUÇÃO DE PROTEÇÃO CONTRA VAZAMENTO E INTEGRIDADE DOS DADOS

7.7.1. Características Básicas da Solução

7.7.1.1. Os equipamentos descritos deverão obrigatoriamente ser de um único fabricante, não podendo se utilizar de fabricantes de terceiros para o Hardware nem para o Sistema Operacional e/ou *Software* que compõe a solução.

7.7.1.2. O Sistema Operacional e/ou *software* do *"Software Appliance*" descrito na premissa inicial deverá ser de um único fabricante e funcionar sobre plataforma de Máquina Virtual suportados na seguinte configuração: VMware vSphere (ESX) 4.x ou superior e/ou VMware vSphere Hypervisor (ESXi) 5.x ou superior.

7.7.1.3. A solução deverá contemplar equipamentos do tipo *Appliance* para os seguintes módulos:

7.7.1.3.1. Monitoramento - Capaz de detectar e monitorar o trafego de rede e estação de trabalho em tempo real;

7.7.1.3.2. Descoberta - Capaz de Detectar, Monitorar e tomar ações em documentos estruturados ou não estruturados em diversas localidades do ambiente protegido:

7.7.1.3.2.1. Compartilhamento de Arquivos;
7.7.1.3.2.2. Banco de Dados; e
7.7.1.3.2.3. Estações de Trabalho.

7.7.1.3.3. Prevenção - Capaz de detectar, monitorar e bloquear determinado documento e/ou conteúdo classificado que saia do ambiente de trabalho através de Protocolos Web e Emails;

7.7.1.3.4. Gerenciamento - Capaz de gerenciar de forma Única e centralizada as regras de todos os equipamentos sem gerar perda de performance e sem a necessidade de múltiplas consoles de gerenciamento.

7.7.2. Característica de Arquitetura Distribuída da Solução

7.7.2.1. Arquitetura multicamada escalável para centenas de servidores de detecção e milhares de agentes de terminal, por servidor;

7.7.2.2. Atualizações de *software* automáticas a partir de um console centralizado para servidores e terminais, inclusive o mesmo servidor será responsável por gerenciar todas as soluções de Monitoramento, Descoberta e Prevenção, sobre as camadas de Rede, *Storage* e Estação de Trabalho.

7.7.3. Característica de Gerenciamento do Sistema

7.7.3.1. Relatórios de tráfego e de desempenho do sistema e indicadores de rendimento máximo;

7.7.3.2. Capacidade de excluir incidentes em lote e eliminar detalhes específicos de incidentes do banco de dados;

7.7.3.3. Enviar alertas em tempo real por e-mail sobre as condições do nível do sistema, Syslog e soluções de SIEM;

7.7.3.4. Deverá possuir um mecanismo de pesquisa dos dados armazenados direto na interface de gerenciamento de fácil acesso e fácil pesquisa tais como: Palavra Chave; Tipo de Documento; Protocolo; Email de Origem e Email de Destino.

7.7.3.5. Criação e customização de Expressões regulares para consultas e pesquisas.

7.7.3.6. Deverá possuir um mecanismo de Disaster Recovery para acesso ao Gerenciamento da Solução e salva guarda dos dados.

7.7.3.7. Acesso ao Sistema e Segurança Mecanismos de criptografia em conformidade total com os padrões de manuseio de dados PCI;

7.7.3.8. Criptografia de dados na captura e salvaguardar dos dados - monitoração e agentes;

7.7.3.9. Armazenamento de dados no banco de dados de incidentes, em formato criptografado;

7.7.3.10. Os canais de comunicação entre componentes do sistema são autenticados e criptografados;

7.7.3.11. Todos os dados indexados são protegidos, mesmo quando criados remotamente;

7.7.3.12. Registros detalhados de auditoria de atividades de transação na solução e Banco de Dados, por usuário e ações executadas;

7.7.4. Características de Regras e Políticas da Solução

7.7.4.1. Detecção – Conteúdo Identificado.

7.7.4.1.1. Capacidade de obter a impressão digital de dados estruturados (Ex. CPFs) e não estruturados (MS Office docx's e doc's, PDFs, código-fonte);

7.7.4.1.2. Capacidade de especificar, exatamente, quais colunas dos dados estruturados em databases (Banco de Dados) identificados são necessárias para localizar uma correspondência (por exemplo, nome, sobrenome e CPF, mas não o CEP);

7.7.4.1.3. Capacidade para detectar, nos documentos não estruturados identificados, as extrações ou derivações dos documentos dentro de um limite percentual definido;

7.7.4.2. Detecção – Conteúdo Descrito

7.7.4.2.1. Detectar em listas personalizáveis de palavras e frases, com a capacidade de incluir palavras-chave múltiplas em uma única regra de detecção e especificar

a proximidade da palavra-chave necessária para estabelecer uma correspondência;

7.7.4.2.2. Capacidade integrada de detectar uma grande variedade de padrões de dados que representam dados confidenciais;

7.7.4.2.3. Informações integradas sobre faixas de números válidos para diferentes tipos de dados Capacidade de excluir, automaticamente, faixas de números inválidos para tipos de dados específicos;

7.7.4.2.4. Capacidade de criar novos padrões de identificação de dados com validadores para números internos de ID, padrões proprietários e assim por diante, bem como, personalizar padrões pré-configurados de identificação de dados;

7.7.4.2.5. Detectar de acordo com expressões regulares totalmente configuráveis;

7.7.4.2.6. Detectar por tipo de arquivo, por nome e extensão de arquivo, atributos do remetente/destinatário e protocolo de transmissão;

7.7.4.2.7. Mais de 60 modelos de política preexistentes que incluem palavras-chave e padrões de dados para as leis americanas e internacionais, incorporando as melhores práticas que podem ser ajustadas com facilidade.

7.7.4.2.8. Detecção baseada em um mecanismo ciente do conteúdo em tempo real, possibilitando a detecção do conteúdo com ou sem uso de marcações (*tagging*).

7.7.4.3. Definição de Política

7.7.4.3.1. Configurar políticas para detectar/configurar limites com base na quantidade de correspondência, de acordo com cada política;

7.7.4.3.2. Criar políticas que combinam várias tecnologias e regras de detecção com regras lógicas (E/OU) e de exceção; Deverá Suportar no mínimo, 512 regras concorrentes Ativas; Definir regras de detecção de grupos com base nas informações internas do diretório, como um departamento ou unidade comercial; Capacidade de integrar diretamente com LDAP e AD para criar regras de detecção baseadas em usuário ou grupo para remetente e destinatário;

7.7.4.3.3. Capacidade de integrar diretamente com LDAP e AD para criar regras de detecção de terminal baseadas em usuário ou grupo. Políticas diferentes podem ser aplicadas de acordo com o usuário que fez o login, mesmo em uma máquina compartilhada;

7.7.4.3.4. Capacidade de exportar/importar facilmente as regras de detecção existentes, incluindo a importação de regras de detecção de diferentes sistemas;

7.7.5. Implementação Automática

7.7.5.1. Envia, automaticamente, notificações personalizadas por e-mail ao funcionário, gerente e administradores.

7.7.5.2. Envia, automaticamente, a mensagem a qualquer sistema de gerenciamento de caso ou de eventos de segurança, com suporte ao Syslog.

7.7.5.3. Configurar várias respostas automáticas com base na severidade, contagem de combinações e política.

7.7.5.4. Acesso com base na função e controle de privacidade.

7.7.5.5. Limita o acesso de incidentes para uma função política, departamento ou unidade comercial, localização, estado de severidade ou solução, ou qualquer atributo personalizado definido pelo usuário;

7.7.5.6. Cria funções separadas para a administração técnica de servidores, administração de usuário, criação e edição de política, solução e exibição de incidentes para dados armazenados ou em uso, estejam na rede ou no terminal;

7.7.6. Fluxo de Trabalho da Reação a Incidente

7.7.6.1. Interface de resposta totalmente personalizável que permite combinações de várias ações de reparo exibe todos os detalhes do incidente em uma única página, permitindo que o usuário, rapidamente, tome uma decisão e a coloque em ação;

7.7.6.2. Capacidade de personalizar, por usuário, tanto o layout quanto os dados em uma imagem (snapshot) do incidente;

7.7.6.3. Armazenar e exibir a mensagem original ou arquivo que gerou o incidente;

7.7.6.4. Facilitar a verificação da correlação entre incidentes por assunto, remetente, destinatário, nome de arquivo, proprietário do arquivo, nome de usuário e política;

7.7.6.5. Exibir todo o histórico do incidente, inclusive as alterações e edições referentes ao mesmo;

7.7.6.6. Resolução da identificação de remetente, usuário da máquina e proprietário do arquivo via LDAP e AD e capacidade de se integrar a essas fontes para identificar a informação e realizar ações como mapear um endereço IP até um nome de usuário e e-mail corporativo;

7.7.6.7. Capacidade de pré-configurar o sistema de modo otimizado para setores verticais específicos, incluindo políticas, relatórios, funções e fluxo;

7.7.7. Relatórios e Análises

7.7.7.1. Interface de usuário baseada em navegador, acessível pelo Internet Explorer e Mozilla Firefox.

7.7.7.2. Relatório de incidentes e tendências por empresa, departamento e usuário, utilizando o diretório corporativo.

7.7.7.3. Relatórios resumidos por níveis como, incidentes agrupados, no mesmo relatório, por unidades comerciais, por políticas e por severidade.

7.7.7.4. Capacidade para agrupar, filtrar e classificar relatórios por diferentes parâmetros, inclusive por departamento ou unidade comercial.

7.7.7.5. Painéis de risco configuráveis que exibem, simultaneamente, diferentes níveis de relatórios de incidentes.

7.7.7.6. Capacidade para configurar e salvar relatórios e painéis personalizados, por usuário.

7.7.7.7. Opção de publicar relatórios salvos para todos os usuários por função ou mantê-los como relatórios pessoais.

7.7.7.8. Capacidade de enviar qualquer relatório por e-mail, sob comando ou via agendamento regularmente definido.

7.7.7.9. Capacidade de exportar os relatórios nos formatos HTML e CSV para exibi-los fora da interface.

7.7.7.10. Possibilidade de executar relatórios em banco de dados, com pelo menos 200.000 incidentes, com impacto mínimo no desempenho.

7.7.7.11. Facilidade de navegação por qualquer relatório, obtendo detalhes adicionais de incidentes sem ter de executar um novo relatório.

7.7.7.12. Fluxo de relatórios antigos para fornecer incidentes em diferentes estados, agrupados por período de tempo.

7.7.7.13. Lista abrangente de relatórios de sistema padrão com capacidade para configurar a lista visível de relatórios do sistema, por usuário.

7.7.8. DLP de Rede e Armazenamento

7.7.8.1. Capacidades de Monitoramento de Múltiplos Protocolos.

7.7.8.2. Monitora o e-mail corporativo usando estações de trabalho, Smartphones e Tablets executando o Google Android, Apple iOS e Windows Mobile; Monitora os seguintes protocolos:

7.7.8.2.1. AOL Instant Messenger;
7.7.8.2.2. BitTorrent;
7.7.8.2.3. Citrix ICA;
7.7.8.2.4. FTP;
7.7.8.2.5. HTTP;
7.7.8.2.6. HTTPS;
7.7.8.2.7. ICY;
7.7.8.2.8. IMAP;
7.7.8.2.9. IRC;
7.7.8.2.10. KaZaA;
7.7.8.2.11. LDAP
7.7.8.2.12. MSN Messenger;
7.7.8.2.13. NTLM;
7.7.8.2.14. PCAnywhere;
7.7.8.2.15. POP3;
7.7.8.2.16. RDP;
7.7.8.2.17. Rlogin;
7.7.8.2.18. RTSP;
7.7.8.2.19. SMB;
7.7.8.2.20. SMTP;
7.7.8.2.21. SOCKS;

7.7.8.2.22. SSH;
7.7.8.2.23. Skype;
7.7.8.2.24. Telnet;
7.7.8.2.25. VNC;
7.7.8.2.26. Yahoo Messenger;
7.7.8.2.27. Windows Live Messenger

7.7.8.3. Capacidade de monitorar protocolos AIM, Yahoo, MSN, além de classificar a passagem do tráfego destes protocolos de MI encapsulado em HTTP;

7.7.8.4. Classifica todos os protocolos, mesmo quando executados em portas que não são padrão;

7.7.8.5. Capacidade para controlar picos de tráfego, tráfego de buffer e fornecer insight em pacotes que não podem ser processados;

7.7.8.6. Capacidade de filtrar o tráfego da rede para inspeção, segundo o protocolo, faixa de IP e remetente/destinatário de e-mail;

7.7.8.7. Fornecer estatísticas de tráfego detalhadas e resultados gerais de dados, nº de mensagens e nº de incidentes, com base em cada protocolo e resumidas de hora em hora; a indexação e captura de todas as informações devem ser independentes das regras aplicadas e da classificação de conteúdo para tal;

7.7.8.8. A Solução de monitoramento, prevenção e descoberta deverão funcionar em alta disponibilidade;

7.7.8.9. A Solução de monitoramento deverá ser capaz de monitorar e armazenar registros de todo o tráfego de protocolos suportados mesmo sem regras de controle de conteúdo ou classificação de documentos auxiliando na criação de regras e gerando evidencias;

7.7.8.10. O Equipamento deverá ser distribuído em modo passivo, sem impactar a rede, utilizando configurações de Spam port no switch, Rspan ou network tap.

7.7.8.11. A solução deverá prover suporte aos seguintes tipos de arquivos:

7.7.8.11.1. Advanced Documents – BDB, CSS, DBF, DBM, DBX, EPS, FrameMaker, HTML, Lotus, PS, Quicken, RichText, SQL, Stockdata, XML;

7.7.8.11.2. Apple Applications – AppleWorks, MacWrite, VCalendar, WriteNow;

7.7.8.11.3. Binary – Binary, LIF, SKR;

7.7.8.11.4. Chat – AOL, MSN, Yahoo;

7.7.8.11.5. Compressed and Archive Formats – BZIP2, BinHex, Compress, EncryptedZip, GZIP, MS Cabinet, RAR, STuffIt, TAR, TNEF, ZIP;

7.7.8.11.6. Engineering Drawings and Designs – AccelPCad, AllegroPCB, AutoCad, BSDL, Catia, DXF, FreeHand, Gerber, MathCad, Mathematica, Matlab, Pagemaker, Photoshop, Solidworks, Spice, TangoPCad, UnigraphicsCad, ViewLogic, Visio, VisualCad;

7.7.8.11.7. Image Files – BMP, GIF, IFF, JPEG, MSMetaFile, MacDraw, MacPaint, PAL, PCX, PICT, PNG, RDIB, SuperPaint, TIFF;

7.7.8.11.8. Languages – Arabic, Chinese, English, French, German, Hebrew, Hindi, Japanese, Korean, Russian, Spanish, Vietnamese;

7.7.8.11.9. Mail – Eudora, IMAP, MIME, MSExchange, MSOutlook, Mail Headers, POP3, RFC822, SMTP, Webmail;

7.7.8.11.10. Microsoft – Money, Password, Registry, Write

7.7.8.11.11. Multi-media Formats – AIFF, ASF, AVI, ICY, MIDI, MIDI-RMI, MP3, MPEG, MPlayer, Movie_ANI, NIFF, QuickTime, RCP, RIFF, RMMP, RTSP, RealMedia, SD2, Shockwave, SoundFont, WAV;

7.7.8.11.12. Office Applications – CSV, Encrypted Documents (Excel, PDF, PowerPoint, Word), Non-encrypted Documents (Excel, PDF, PowerPoint, Word), WordPerfect

7.7.8.11.13. Other Types – ASCII, CAP, CMS, CVS, PCAP, iGaming;

7.7.8.11.14. P2P – BitTorrent, DirectConnect, Gnutella, Kazaa, MP2P, Sherlock, WinMX, eDonkey, eMule;

7.7.8.11.15. Protocol – Citrix, Crypto, FTP, HTTP, HTTPS, ICQ, IMAP, IRC, LDAP, PCAnywhere, POP3, RDP, RPC, SMB, SMTP, SSH, Skype, Telnet, VNC;

7.7.8.11.16. Source Code – Ada, Assembly, Brew, Basic, C, C++, Cobol, Fortran, Java, Lisp, Pascal, Perl, Python, Think C, Think Pascal, VHDL, Verilog, XQuery;

7.7.8.11.17. UNIX – Bash, Bourne, C Shell, K Shell;

7.7.8.12. Os equipamentos de descobrimento de documentos na rede devem suportar pelo menos os seguintes tipos de repositórios:

7.7.8.12.1. CIFS (Windows laptops, desktops, servers, UNIX/Linux/Mac via SAMBA);

7.7.8.12.2. NFS (UNIX/Linux/Mac servers);

7.7.8.12.3. HTTP (internet/intranet, wikis, blogs);

7.7.8.12.4. HTTPS (SSL internet/intranet, wikis, blogs);

7.7.8.12.5. FTP (file transfer servers);

7.7.8.12.6. FTPS (secure file transfer servers);

7.7.8.13. E Nos Seguintes Banco de Dados: MS SQL, Oracle, DB2 e MySQL Enterprise

7.7.8.14. O equipamento de descobrimento deve suportar vários tipos de sistemas NAS incluindo NetAPP.

7.7.8.15. O sistema de descobrimento de documentos deve suportar todos os repositórios listados anteriormente sem a necessidade de agente ou cliente adicional.

7.7.8.16. O sistema de descobrimento deve ser capaz de detectar sistemas de criptografia e tentar acessar estes documentos assumindo as credenciais oferecidas pelo administrador na configuração de varredura.

7.7.8.17. O sistema de varredura dos sistemas de descobrimento deve ser feita de forma incremental e deve ser capaz de comparar possíveis modificações nos documentos detectados.

7.7.8.18. O sistema de descobrimento deve ser capaz de operar em alta disponibilidade.

7.7.8.19. O sistema deve ser capaz de detectar a relação de classificação de elementos de forma individual por proximidade gerando incidentes em documentos desconhecidos por classificação de conteúdo.

7.7.8.20. O equipamento de descobrimento deve ter funcionalidade de controle de banda para copia e varredura de rede em busca de documentos confidenciais.

7.7.8.21. Possuir pelo menos dois mecanismos de monitoramento de documentos registrados, através de web upload, ou seja, upload de arquivo ou registro de scans;

7.7.8.22. Sistema de descoberta escalável, ou seja, o documento registrado que não esta sendo utilizado fica sendo monitorado mesmo que modificado;

7.7.8.23. O produto devera suportar pelo menos 1 milhão (1.000.000) de documentos registrados;

7.7.8.24. Cada equipamento devera suportar pelo menos 1GB de conteúdo assinado, ou marcado com tag;

7.7.8.25. O equipamento devera ser capaz de fornecer toda sua classificação em memória não comprometendo a performance do produto;

7.7.8.26. A Solução deve suportar analise léxica de documentos;

7.7.8.27. O sistema de prevenção de rede deve suportar o bloqueio de SMTP, HTTP, HTTPS, FTP e Instant Messaging.

7.7.8.28. O sistema de prevenção de rede deve tomar as seguintes ações: Email de notificação, Notificação via Syslog, Aplicar uma Análise e Aplicar um Status.

7.7.8.29. O sistema de prevenção de Emails deve tomar as seguintes ações: Bloquear, Encryptar, Notificar, Guardar em Quarentena e Redirecionar.

7.7.9. Capacidades de Carga e Captura.

7.7.9.1. Monitora linhas de velocidade gigabit sem perda de pacotes para compensar carga excessiva;

7.7.9.2. Capacidade de Captura de até 500Mbps sem uso de hardware de rede (NIC) especifico;
7.7.9.3. Capacidade de capturar todo o tráfego monitorado sem a necessidade de criação de políticas fazendo com o que todos os dados de um segmento ou domínio sejam passiveis de analise e auditoria futura;

7.7.9.4. Não requer o uso de MTA ou *proxy* web incorporados, possibilitando usar os melhores produtos existentes, devem, respectivamente, funcionar com os protocolos ICAP e SMTP *Relay*;

7.7.9.5. Uma notificação automática, via e-mail, pode ser enviada ao usuário e gerente durante a ocorrência de um incidente;

7.7.9.6. Capacidade de Indexação de pelo menos 35 milhões de documentos por módulo;

7.7.9.7. A solução deverá ser totalmente capaz de integração futura, adequando as características de bloqueio utilizando *Appliances* e/ou *Software Appliances* interligados a *gateway* de email e

web, bem como o monitoramento, descoberta e bloqueio em Banco de Dados Relacionais e de dados estruturados;

7.7.10. Características de *Hardware* (*Appliances*)

7.7.10.1. No caso do contratante optar por qualquer um dos módulos citados como *Appliance*, ou seja, a união de *Hardware* e *Software*, o mesmo deverá ter as seguintes configurações:

7.7.10.1.1. Ser de um mesmo Fabricante;

7.7.10.1.2. Ter, no mínimo, 2 placas para captura 10/100/1000 (Metálico ou Fibra Óptica) para captura de dois segmentos distintos;

7.7.10.2. O Hardware deverá ser fornecido com as seguintes características físicas mínimas:

7.7.10.2.1. Fontes de alimentação redundantes padrão Hot Swap; 3 módulos de rede ethernet 10/100/1000; Controlador Raid1/Raid5; 8 unidades de Discos padrão Sata 7200rpm com 2TB de capacidade de armazenamento; 32GB de Memória RAM; 2 x CPU Intel Xeon com no mínimo 2,0Ghz e 6 cores de Processamento; Capacidade de Gerenciamento remoto RMM;

7.7.11. DLP de Terminal (Agente)

7.7.11.1. Cobertura:

7.7.11.1.1. Descoberta, baseada em agente, de dados confidenciais em terminais, incluindo relatórios sobre as listas de controle de acesso para os arquivos que violam as políticas;

7.7.11.1.2. O agente oferece cobertura completa estando a máquina dentro ou fora da rede;

7.7.11.1.3. O agente armazena em cache os arquivos que causaram o incidente até que o usuário se conecte, novamente, à rede corporativa;

7.7.11.2. Cobertura da Ação do Usuário:

7.7.11.2.1. Monitorar dados descarregados na unidade local;

7.7.11.2.2. Monitorar e bloquear dados copiados para dispositivos de armazenamento removível dos tipos USB, *Firewire*, cartões de memória SD e flash;

7.7.11.2.3. Definir dispositivos removíveis individuais, ou grupos de dispositivos, como confiáveis e criar exceções de políticas para esses dispositivos;

7.7.11.2.4. Criptografar, automaticamente, os dados confidenciais ao copiá-los para um dispositivo USB;

7.7.11.2.5. Monitorar e bloquear dados copiados para CD/DVD;

7.7.11.2.6. Monitorar e bloquear e-mail corporativo (webmail) ;

7.7.11.2.7. Monitorar e bloquear transmissões HTTP;

7.7.11.2.8. Monitorar e bloquear transmissões de mensagens instantâneas pelo Yahoo, MSN e AOL;

7.7.11.2.9. Monitorar e bloquear transmissões via FTP;

7.7.11.2.10. Monitorar e bloquear dados enviados a qualquer tipo de impressora local e de rede;

7.7.11.2.11. Monitorar e bloquear dados enviados a um fax local e de rede;

7.7.11.2.12. Monitorar e bloquear ações de copiar e colar feitas através da área de transferência do Windows;

7.7.11.2.13. Monitorar e bloquear dados copiados para, e a partir de, compartilhamentos de rede pelo Windows Explorer;

7.7.11.2.14. Monitorar e bloquear o uso de dados confidenciais por qualquer aplicativo, incluindo programas de criptografia não autorizados e aplicativos com protocolos proprietários. Possuindo como cobertura do fabricante para Skype, Webex, LiveMeeting, Office Communicator, Bluetooth;

7.7.11.2.15. Bloquear ações de captura de tela com base no conteúdo;

7.7.12. Implementação e Gerenciamento do Agente

7.7.12.1. O agente deve ser suportado no mínimo nos Seguintes Sistemas Operacionais Microsoft: Windows XP Profissional SP3 ou superior, Windows Vista SP2 ou superior, Windows 7 SP1, Windows 8 ou 8.1, Windows Server 2003 SP2, Windows Server 2003 R2, Windows Server 2008 SP2, Windows Server 2008 R2 SP1 ou superior, Windows Server 2012 R2 64-bit.

7.7.12.2. O agente deve ser suportado no mínimo nos Seguintes Sistemas Operacionais Apple: OS X Lion 10.7.5 ou superior, OS X Mountain Lion 10.8.0 ou superior, OS X Mavericks 10.9.0.

7.7.12.3. O agente deverá ser suportado no mínimo nos sistemas virtualizados:

7.7.12.3.1. Sistemas VDI: Citrix XenDesktop 5.5, 5.6, e 7.0, VMware View 4.6, 5.0, 5.1 e 5.2;

7.7.12.3.2. Desktops remotos: Citrix XenApp 6.0, 6.5 com “Feature Pack 2”, Microsoft Remote Desktop;

7.7.12.4. A Gerência do Data Loss Prention deverá ser responsável pela Distribuição (*Deploy*), Instalação, Gerenciamento e Desinstalação do Agente nas estação, bem como deverá executar inventário das maquinas nas quais estão com agentes instalados, esse inventário deverá coletar informações cruciais para o uso ideal do agente de DLP na estação do usuário;

7.7.12.5. Essa instalação poderá ser remota de forma silenciosa e sem a intervenção do usuário.

7.7.12.6. Um único agente executa todas as funções, inclusive a verificação de terminais e a monitoração e bloqueio de dados que saem do terminal.

7.7.12.7. Define limites em % de uso do processador e disco e a quantidade de largura de banda utilizada pelo agente, minimizando o impacto no terminal e na rede.

7.7.12.8. Integra-se com os *drivers* do sistema operacional Windows em várias aplicações para garantir a estabilidade, interoperabilidade e segurança.

7.7.12.9. Utiliza um console de gerenciamento de agente dedicado e desenvolvido para fins de implementação e gerenciamento e integrado a toda a estrutura/console de gerenciamento da solução *Endpoint*;

7.7.12.10. Implementa agente no alvo por grupos do LDAP e AD;

7.7.12.11. Aplica diferentes configurações de agente, cobrindo diferentes ações de usuário, a agentes individuais e grupos de agentes;

7.7.12.12. Suporta ferramentas de solução de problemas e de diagnóstico de agente criadas para usuários que não são da TI;

7.7.12.13. Gerencia a reinicialização e desligamento do agente, ativação e desativação do agente, recuperação de registros, alertas e configuração pelo console central;

7.7.12.14. Orienta agentes para servidores e terminais diferentes, a qualquer momento e configura os agentes para redirecionamento ao servidor secundário, se o primário não estiver disponível;

7.7.12.15. Opções adicionais para gerenciamento centralizado de implementação e atualização de software e definição dos níveis de registro;

7.7.12.16. Possibilitar o uso de chave de desbloqueio de documentos através do sistema de *challenge response*. A chave deve ser gerada pelo administrador do sistema;

7.7.12.17. Escalabilidade:

7.7.12.17.1. A verificação com base em agente permite verificações paralelas de milhares de terminais;

7.7.12.17.2. Capacidade de proteger grandes volumes de dados, como bancos de dados completos de registros de usuário, grande quantidade de documentos identificados.

7.7.12.18. Segurança do Agente:

7.7.12.18.1. O agente não é exibido na lista "Adicionar ou remover programas", nem na bandeja do sistema e permanece invisível no painel Serviços e no Gerenciador de Tarefas;

7.7.12.18.2. As comunicações entre o agente e o servidor são criptografadas e autenticadas;

7.7.12.18.3. Opção de solicitação de senha para desinstalar o agente;

7.7.12.19. Gerenciamento de Verificação e Ações de Proteção de Dados:

7.7.12.19.1. Capacidade para configurar e controlar todas as verificações a partir de um único console centralizado;

7.7.12.19.2. Configurar verificações incrementais nas quais apenas arquivos novos e alterados sejam verificados;

7.7.12.19.3. Os agentes informam o progresso para uma localização central, permitindo que haja relatórios de progresso atualizados enquanto as verificações são executadas;

7.7.12.19.4. Capacidade para executar verificações de filtro com base no tamanho, tipo e local do arquivo;

7.7.12.19.5. Capacidade de verificar e executar somente quando a máquina estiver ociosa, eliminando assim qualquer impacto negativo na máquina;

7.7.12.19.6. Capacidade de colocar arquivos confidenciais em quarentena no terminal, e em outro ponto da rede;

7.7.12.20. Capacidade de Customização e gerenciamentos dos itens:

7.7.12.20.1. Utilização de CPU e memória;

7.7.12.20.2. Utilização de largura de banda das interfaces de rede;

7.7.12.20.3. Disponibilidade de cada componente da solução, medido através de *pooling* SNMP ou PING.

7.7.12.21. Na tela, notificações *pop-up* com campos para justificativa do usuário podem ser exibidas durante a ocorrência de um incidente.

7.7.12.22. Opção de resolução automática para usuário de terminal, notificando na tela pedindo ao usuário para confirmar ou cancelar a transferência de dados confidenciais.

7.7.12.23. Uma notificação automática, via e-mail, pode ser enviada ao usuário e gerente durante a ocorrência de um incidente.

7.7.12.24. Impõe, automaticamente a criptografia de arquivos confidenciais ao copiar para dispositivos removíveis, como dispositivos USB, *FireWire* como também diretórios de rede compartilhados.

7.7.12.25. Deve possuir integração com ferramentas de criptografia para aplicação da mesma, caso seja esta a ação definida pelo administrador da solução.

7.7.12.26. A solução de criptografia do item anterior deverá ser a mesma do DLP e não será permitido adequar integração em gerências em separado da solução global de DLP, do Antivírus, Host IPS e *Firewall* de Estação;

7.7.12.27. A solução deve possuir integração com ferramentas de gerenciamento de direitos no arquivo para aplicação da mesma caso seja esta a ação definida pelo administrador da solução;

7.7.12.28. A integração de gerenciamento de direitos no arquivo deverá ser compatível com pelo menos uma das soluções de mercado a seguir: Adobe LiveCycle Rights Management, Microsoft Rights Management System, Oracle Information Rights Management.

7.7.13. Solução de Criptografia de Disco e Conteúdo

7.7.13.1. A Solução de criptografia deve suportar ao menos os seguintes sistemas operacionais: Windows Server 2012, Windows Server 2008, Windows Server 2003, Windows 10, Windows 8.1, Windows 7, Windows Vista, Windows XP e Windows XP Home Edition.

7.7.13.2. Para o módulo de gerencia de criptografia nativa devem ser suportados os Sistemas Operacionais Apple Yosemite 10.10, Apple Mavericks 10.9.x e Apple Mountain Lion 10.8.x.

7.7.13.3. A solução de criptografia deve ter a capacidade de criptografar todo o disco rígido com criptografia AES-256 bit;

7.7.13.4. A solução de criptografia deve ter a capacidade de implementar autenticação pré-boot.

7.7.13.5. A solução de criptografia deve ter a capacidade de registrar automaticamente o usuário para o Windows após a autenticação bem-sucedida de pré-boot.

7.7.13.6. A solução de criptografia deve ter a capacidade de manter as senhas entre o Windows e pré- boot sincronizadas.

7.7.13.7. A solução de criptografia deve ter a capacidade de ser gerenciada de forma centralizada a partir da mesma console de gerenciamento da solução antivirus ofertada.

7.7.13.8. A solução de criptografia deve ter a capacidade de automaticamente guardar (backup) as chaves de recuperação.

7.7.13.9. A solução de criptografia deve criar uma chave de criptografia exclusiva para cada máquina.

7.7.13.10. A solução de criptografia deve ter a capacidade de recuperar dados a partir de uma máquina sem descriptografar o disco.

7.7.13.11. A solução de criptografia deve ter a capacidade de redefinir senhas remotamente.

7.7.13.12. A solução de criptografia deve ter a capacidade de redefinir senhas localmente.

7.7.13.13. A solução de criptografia deve ter a capacidade de impedir que o usuário descriptografe o disco e remova/desinstale o software.

7.7.13.14. A solução de criptografia deve ter certificação FIPS.

7.7.13.15. A solução de criptografia deve ter a capacidade de comunicar/reportar centralmente o estado de encriptação de cada máquina.

7.7.13.16. A solução de criptografia deve ter a capacidade de criar acesso baseado em função granular (*role-based access*).

7.7.13.17. A solução de criptografia deve ter a capacidade de gerenciar múltiplas plataformas a partir da mesma console de gerenciamento.

7.7.13.18. A solução de criptografia deve ter a capacidade de personalizar a aparência do ambiente de autenticação de pré-boot.

7.7.13.19. A solução de criptografia deve ter a capacidade de atribuir automaticamente os usuários de pré-boot no sistema.

7.7.13.20. A solução de criptografia deve ter a capacidade de desativar temporariamente a autenticação de pré-boot via política.

7.7.13.21. A solução de criptografia deve ter a capacidade de desativar temporariamente a autenticação de pré-boot através de um CLI local.

7.7.13.22. A solução de criptografia deve ter a capacidade de detectar hardwares não compatíveis antes da ativação.

7.7.13.23. A solução de criptografia deve ter a capacidade de executar uma inspeção prévia sobre a saúde do disco antes da ativação.

7.7.13.24. A solução de criptografia deve ativar a tecnologia de criptografia Intel AES-NI, quando disponível.

7.7.13.25. A solução de criptografia deve ter Opções de Acessibilidade para os deficientes visuais.

7.7.13.26. A solução de criptografia deve ter a capacidade de ativar funcionalidade tipo "bomba-relógio" em máquinas que tiverem sido desconectadas da rede corporativa por tempo determinado pelo administrador.

7.7.13.27. A solução de criptografia deve ter a capacidade de atribuir usuários e grupos do *Active Directory* para máquinas.

7.7.13.28. A solução de criptografia deve ter a capacidade de implementar o agente através da console de gerenciamento ou através de *software* terceiro de distribuição.

7.8. SERVIÇO DE GESTÃO DE EVENTOS E INCIDENTES

7.8.1. Características Básicas da Solução

7.8.1.1. A solução deve ser composta de software embarcado em hardware no formato *Appliance*, homologados e fornecidos pelo fabricante para todos os componentes da solução.

7.8.2. Características Gerais da Solução

7.8.2.1. O sistema operacional da solução deve ser mantido pelo próprio fabricante.

7.8.2.2. Deve utilizar para armazenamento e gerenciamento das informações coletadas, base de dados integrada em cada um dos dispositivos da solução (caso esta seja ofertada em mais de um *Appliance*), proprietária e inteiramente desenvolvida e suportada pela empresa, não sendo aceitas soluções baseadas em base de dados Open Source tais como MySQL, PostgreSQL e mSQL, e que não exija conhecimentos específicos de bancos de dados para sua manutenção.

7.8.2.3. A solução deve ser composta pelo menos pelos seguintes componentes: coletor, correlacionamento, gerenciamento e armazenamento;

7.8.2.4. Arquitetura da solução deve ser escalável, suportando crescimento da quantidade de ativos, eventos, Data Center ou localidades remotas, a partir da aquisição de licenças ou componentes de correlacionamento, armazenamento ou coleta, sem a necessidade de troca ou aquisição do componente de gerenciamento;

7.8.2.5. O licenciamento da solução deve ser através do número de eventos por segundo, permitindo a livre distribuição de coletores, ou solução similar, independente de número e arquitetura.

7.8.2.6. Sendo o licenciamento da solução por número de eventos por segundo, a licença deve permitir o recebimento de eventos de número ilimitado de ativos, observando o limite de eventos por segundo.

7.8.2.7. A solução deverá suportar um total de no mínimo 1.200 eventos por segundo de forma contínua e não limitada em caso de picos eventuais, oriundos dos seguintes, e não limitados aos ativos de segurança listados neste Termo de Referência.

7.8.2.8. Deverá ser fornecido junto à solução de SIEM, suporte de manutenção de 48 MESES que contemple suporte para todo o sistema (*hardware*, *software*, módulos e licenciamento), atualização de *firmware*, *patches* corretivos e atualizações de versões.

7.8.2.9. Cada *Appliance* da solução deve:

7.8.2.9.1. Estar em conformidade com as seguintes certificações de hardware:
7.8.2.9.2. Common Criteria EAL3 e FIPS 140-2 Level 2;
7.8.2.9.3. Possuir no mínimo 2 discos redundantes para armazenamento dos dados;
7.8.2.9.4. Possuir duas fontes redundantes de energia;

7.8.2.10. A comunicação entre os diversos módulos e *Appliances* da solução deverá ser realizada de forma segura utilizando para isso canal criptografado com algoritmo AES-256;

7.8.2.11. A solução deve ser capaz de receber diferentes tipos de formato de fluxo de redes, tais como *netflow*, *sflow*, e ainda assim, ser capaz de gerar fluxos de rede automaticamente mediante a captura de informações na rede em interface de coleta especifica em modo promiscuo;

7.8.2.12. A solução deverá prover a funcionalidade de monitoramento em tempo real, tais como:

7.8.2.12.1. *Baselining* dinâmica de eventos para detecção de anomalia;
7.8.2.12.2. Correlação de eventos baseadas em regras e em riscos;
7.8.2.12.3. Análise comportamental e Análise de tráfego de rede (*flow*) de todos os dispositivos de segurança, *switches*, *routers* e todos os servidores Windows e Unix;

7.8.2.13. Deve prover mecanismos para notificar problemas na solução de forma proativa, informando ao administrador sobre a alta utilização de recursos do sistema via SNMP e na interface de gerenciamento da solução;

7.8.2.14. A solução deve suportar IPv6;

7.8.2.15. Deve possuir um *baseline* comportamental da rede, definido por suas regras e correlações, fornecendo alertas sempre que ocorrer algum evento fora do comportamento normal. Este *baseline* deve ser executado em *realtime*, mesmo tendo como linha de base mais de 1 (um) mês de dados;

7.8.2.16. Deve permitir o correlacionamento de eventos e alertas com dados existentes em listas (*watchlist*), e também a criação de novas listas, além da edição das existentes, tanto de forma automatizada quanto manual. Deve permitir a criação de listas estáticas ou dinâmicas;

7.8.2.17. Com o resultado de regras, deve ser capaz de executar ações automáticas como: executar script, enviar e-mail, enviar SMS e enviar mensagem para o usuário conectado no console;

7.8.2.18. Popular uma lista estática ou dinâmica, onde nestas listas pode adicionar ou remover automaticamente dado de determinado evento.

7.8.2.19. Deve possuir módulo que permita análise de risco em atividades realizadas na sua rede.

7.8.2.20. O risco relativo de cada atividade, deve ser calculado com base em valores atribuídos pelo cliente.

7.8.2.21. Todo e qualquer ativo pode receber um “peso”, que será utilizado nos cálculos de risco.

7.8.2.22. Além dos ativos, outros itens poderão receber diferentes “pesos”. Por exemplo: permissões de usuário, ações realizadas (alteração de arquivos, configurações da máquina), tipo de documento, entre outras.

7.8.2.23. Deve suportar múltiplos mecanismos de correlação e os eventos correlacionados provenientes destes, para execução de atividades de correlação localizada e centralizada.

7.8.2.24. A base de conhecimento de atividades anômalas da internet deve ser alimentada por amostras de pelo menos 100 milhões de nós, distribuídos por pelo menos 120 países.

7.8.2.25. As amostras devem possuir comprovadamente caráter multivetorial, ou seja, deve considerar amostras de produtos de *antimalware*, IPS de rede, *Firewall*, Antispam, filtros de conteúdo, analise e controle de aplicativos e análise de vulnerabilidades.

7.8.2.26. A base de dados de ameaças contida na nuvem, deve ser mantida por equipe de pelo menos 350 pesquisadores, em pelo menos 26 laboratórios ao redor do mundo, sendo essa equipe trabalhando em regime 24x7x365.

7.8.2.27. Esse laboratório deve publicar, sempre que necessário,relatórios tratando de ameaças específicas de grande impacto e/ou tendências de ameaça, bem como recomendações de medidas de proteção.

7.8.2.28. A solução deve ser capaz de descobrir ativos de rede através de varredura ativa.

7.8.2.29. Deve prover serviços de geolocalização para log, eventos e fluxo (*flow*) de rede.

7.8.2.30. A solução deve ser capaz de monitorar dispositivos de rede e prover alertas e auditoria em caso de alteração de configurações.

7.8.2.31. A solução deve incluir editor gráfico de regras de correlação.

7.8.2.32. A solução deve suportar arquitetura redundante para o sistema central de gerenciamento, e todo ambiente redundante (software e hardware) deve ser suportado pela fabricante, não sendo aceito softwares de terceiros objetivando redundância da solução;

7.8.2.33. Deve ser suportada arquitetura distribuída, composta, caso seja necessário, sistemas de gerenciamento hierárquico;

7.8.2.34. Deve possuir funcionalidade de criação de *baseline* dinâmico para todos os endereços IP’s, usuários, hosts, domínios, portas e protocolos.

7.8.2.35. A solução deve disponibilizar capacidade de 3 (três) *Terabytes* de armazenamento para retenção de logs cru ("*raw*"), compreendendo compressão de pelo menos 16:1, chegando ate 20:1;

7.8.2.36. A solução deve ser capaz de armazenar 7 dias de eventos para acesso imediato (online);

7.8.2.37. Deve ser possível adicionar capacidade extra de armazenamento através de dispositivos de *storage* NAS ou SAN, sem a necessidade de aquisição de novos módulos da solução, podendo ainda ser utilizada solução de *storage* pré-implementada no ambiente do BANPARÁ;

7.8.2.38. A coleta dos *logs* e eventos não deverá depender da utilização de agentes ou softwares coletores de terceiros, dentre os métodos de coleta deve ser possível alem dos convencionais *syslog*, um mesmo dado pode ser buscado em sua origem por NFS, SCP, SFTP, HTTP ou FTP;

7.8.2.39. Deve armazenar os eventos, alertas e incidentes na base de dados da solução;

7.8.2.40. O somatório dos valores definidos como peso, em cada uma dessas ações, permitirá a definição do nível de risco inerente a essa atividade.

7.8.2.41. As atividades devem ser separadas em pelo menos 5 níveis de risco para a empresa: Risco muito alto, alto, médio, baixo e muito baixo.

7.8.2.42. Esse módulo também pode permitir a segregação de funções de gerenciamento, correlação em tempo real, correlação histórica, relatórios e interface de acesso entre um ou mais *Appliances*, permitindo uma utilização mais racional da performance total das caixas.

7.8.2.43. A funcionalidade de monitoramento de bancos de dados deverá:

7.8.2.43.1. Rastrear usuários nos aplicativos.
7.8.2.43.2. Examinar toda a atividade da sessão, do logon ao logoff.
7.8.2.43.3. Detectar dados confidenciais e identificar violações de políticas.
7.8.2.43.4. Detectar perda de dados em canais autorizados.
7.8.2.43.5. Correlacionar a atividade de banco de dados a eventos de segurança.
7.8.2.43.6. Gerar relatórios detalhados para PCI DSS, HIPAA, NERC-CIP, FISMA, GLBA, SOX e muitos outros requisitos de conformidade.

7.8.3. Característica de Gerenciamento da Solução.

7.8.3.1. Todas as ferramentas necessárias para o gerenciamento da solução deverão estar disponíveis através de uma única console gráfica acessível via WEB, acessível através de navegadores padrões de mercado, tais como Microsoft Internet Explorer, Firefox Mozilla, Apple Safari ou Google Chrome, e sem a necessidade de acessar diferentes componentes da solução.

7.8.3.2. A solução deve ser integrável com o Microsoft Active Directory (AD) para autenticação e mapeamento de grupo de usuários e suas permissões.

7.8.3.3. Deve permitir o upgrade de licenciamento sem gerar de forma alguma interrupções na coleta de dados.

7.8.3.4. Deve ser permitida a criação de *parsers* (interpretadores) customizados e desenvolvidos através do uso de expressões regulares.

7.8.3.5. Deve-se permitir diferentes configurações de regras de permissão de acesso para diferentes tipos de administradores.

7.8.3.6. A gestão deverá ser realizada através de uma única console de gerenciamento, centralizada.

7.8.3.7. A solução deve prover de forma nativa, sistema de gerenciamento de tickets (chamados).

7.8.3.8. Os alertas e notificações devem ser enviados ao administrador via email, SNMP e *syslog*.

7.8.3.9. A atualização da base de conhecimento sobre atividades maliciosas do sistema de inteligência em nuvem deve possuir periodicidade, no mínimo, diária.

7.8.3.10. A solução deve incluir ferramenta gráfica para edição e elaboração de relatórios.

7.8.3.11. Deve possuir *website* para consulta de reputação de páginas da web, endereços IP suspeitos, servidores de e-mail.

7.8.3.12. Deve possuir página para reportar novas detecções e endereços IP com reputação maliciosa detectados pelo cliente.

7.8.4. Características de Integração com a Solução de Proteção de Terminais e IPS

7.8.4.1. Deve ser capaz de automaticamente aplicar *tags* de classificação nos ativos que sejam visualizados na console de gerenciamento do *Endpoint*;

7.8.4.2. Deve ser capaz de adicionar endereços IPs em quarentena na solução IPS com base em eventos correlacionados pela solução SIEM;

7.9. SOLUÇÃO DE PROTEÇÃO À AMEAÇAS AVANÇADAS, DIRECIONADAS E DO DIA ZERO (ZERO-DAY)

7.9.1. Arquitetura de Hardware

7.9.1.1. Possui política de garantia de um ciclo de vida de no mínimo 3 (três) anos, isto é, após ser anunciado o término da comercialização do equipamento o suporte (End-of-Support) deverá permanecer por no mínimo 3 (três) anos.

7.9.1.2. Baseado em *Appliance Box* suportando montagem em *rack* (bastidor) de 19" (dezenove polegadas), com utilização de 2-RU (02 (dois) rack units – 02 (duas) unidades de bastidor) de altura.

7.9.1.3. Baseado em arquitetura específica e desenvolvido, tanto software quanto hardware, para a funcionalidade única, exclusiva e específica de APT – Advance Persistent Treath, não sendo um equipamento de uso geral e/ou multifuncional (UTM – Unified Threat Management), tal como: Chassi servidor (Server Chassis), Estação de trabalho (Desktop) e/ou Equipamento Blade.

7.9.1.4. Possui armazenamento interno tanto em SSD (Solid State Disk) quanto em HDD (Hard Disk Drive), sendo sua configuração mínima:

- 7.9.1.4.1. 4 (quatro) unidades de HDD com capacidade de no mínimo 4TB (quatro terabytes) de armazenamento interno.
- 7.9.1.4.2. Duas (2) unidades de SSD com capacidade de no mínimo 800GB (oitocentos gigabytes) de armazenamento interno.
- 7.9.1.4.3. Possui capacidade de memória interna de no mínimo 256GB (Duzentos e cinquenta e seis gigabytes).

7.9.1.5. Suportar fonte de energia para Corrente Alterna ou Alternada (AC – Alternating Current).

7.9.1.6. Suportar fonte de energia com chaveamento automático e capacidade de operação em 100V à 240V (50/60Hz) em Corrente Alterna ou Alternada (AC – Alternating Current), com consumo de energia elétrica de 4 x 1.600W.

7.9.1.7. Suportar redundância de fonte de energia "hot swappable/hot pluggable".

7.9.1.8. Suportar dissipação de calor do equipamento de 2 (dois) BTU/hr (British Thermal Unit per hour – Unidade Térmica Britânica por hora).

7.9.1.9. Possui no mínimo as seguintes certificações de segurança (Safety Certification): UL 1950, CSA-C22.2 No. 950, EN-60950, IEC 950 e EN 60825.

7.9.1.10. Possuir no mínimo as seguintes certificações de interferência eletromagnética ("Electromagnetic Interference Certification" ou "EMI Certification"): FCC Part 15, Class A (CFR 47) (USA), ICES-003 Class A (Canada), EN55022 Class A (Europe) e CISPR22 Class A (Int'l).

7.9.2. Desempenho e Escalabilidade

7.9.2.1. Possuir a capacidade de armazenar, no próprio equipamento, máquinas virtuais – também conhecidas como "sandboxes" – simulando ambientes para detecção de ameaças (malwares), sem necessidade de interação com sistemas externos para simular ambientes.

7.9.2.2. Possuir a capacidade de criação de até 60 (sessenta) máquinas virtuais (*sandboxes*) únicas, para detecção de ameaças (*malwares*).

7.9.2.3. Possuir a capacidade de configuração de cluster (múltiplos equipamentos), permitindo:

7.9.2.3.1. Balanceamento de carga para submissão de arquivos.
7.9.2.3.2. Configuração de alta-disponibilidade com nós secundários.
7.9.2.3.3. Criação de cluster de até dez (10) nós de cluster, incluindo o nó primário e os nós secundários.
7.9.2.3.4. Utilização de equipamentos heterogêneos (diferentes modelos) ou homogêneos (um único modelo).

7.9.2.4. Suporta no mínimo seis (6) sistemas operacionais, para criação de máquinas virtuais (*sandboxes*), tais como:

7.9.2.4.1. Microsoft Windows XP:

7.9.2.4.1.1. 32-bit Service Pack 2
7.9.2.4.1.2. 32-bit Service Pack 3

7.9.2.4.2. Microsoft Windows 7:

7.9.2.4.2.1. 32-bit Service Pack 1
7.9.2.4.2.2. 64-bit Service Pack 1

7.9.2.4.3. Microsoft Windows Server 2003:

7.9.2.4.3.1. 32-bit Service Pack 1
7.9.2.4.3.2. 32-bit Service Pack 2

7.9.2.4.4. Microsoft Windows Server 2008 R2:

7.9.2.4.4.1. Service Pack 1

7.9.2.4.5. Microsoft Windows 8:

7.9.2.4.5.1. 32-bit
7.9.2.4.5.2. 64-bit.

7.9.2.4.6. Microsoft Windows 10:

7.9.2.4.6.1. 32-bits
7.9.2.4.6.2. 64-bits

7.9.2.4.7. Microsoft Windows Server 12

7.9.2.4.8. Android:

7.9.2.4.8.1. 2.3
7.9.2.4.8.2. 4.3

7.9.2.5. Suporta a utilização de ambiente operacional comum (COE – Common Operating Environment) como imagem para máquinas virtuais (sandboxes) customizadas.

7.9.2.6. Suporta recriação automática de máquinas virtuais (*sandboxes*) quando houver atualização de versão do software (firmware) do equipamento.

7.9.2.7. Suporta no mínimo dez (10) tipos de arquivos, para detecção de ameaças (*malwares*), tais como:

7.9.2.7.1. Portable Executable 32-bit (.exe, .dll, .scr, .ocx, .sys, .com, .drv, .cpl)
7.9.2.7.2. Microsoft Office (.doc, .docx, .xls, .xlsx .ppt, .pptx, .rtf, CDF V)
7.9.2.7.3. PDF
7.9.2.7.4. Compressed Files (.zip, .rar)
7.9.2.7.5. Android Application Package (.apk)
7.9.2.7.6. Java Archives (JAR)
7.9.2.7.7. JPEG
7.9.2.7.8. PNG
7.9.2.7.9. GIF
7.9.2.7.10. Adobe Flash files (SWF)

7.9.2.8. Suporta a instalação de no mínimo quatro (4) aplicações (programas) nas máquinas virtuais (sandboxes), para detecção de ameaças (malwares), tais como:

7.9.2.8.1. Microsoft Internet Explorer versões 8, 9 ou superior.
7.9.2.8.2. Mozilla Firefox versões 20, 21 ou superior.
7.9.2.8.3. Microsoft Office versões 2003, 2007, 2010 e 2013.
7.9.2.8.4. Acrobat Adobe Reader versões 9, 10 ou superior.

7.9.2.9. Suporta até 250.000 (Duzentos e cinquenta mil) objetos analisados por dia, para detecção de ameaças (malwares).

7.9.2.10. Possui uma (1) interface exclusiva e dedicada para gerência.

7.9.2.11. Possui uma (1) interface serial (padrão “RJ45 serial-A port”) exclusiva e dedicada para console.

7.9.3. Modos de Implantação/Operação

7.9.3.1. Suporta, de forma homogênea e heterogênea, as seguintes opções de implantação/operação em um único equipamento:

7.9.3.1.1. Standalone:

7.9.3.1.2. Integração nativa com Solução de Prevenção de Intrusos deste Termo de Referência;

7.9.3.1.3. Integração nativa com Solução de *Gateway* de Email e Web deste Termo de Referência;

7.9.3.1.4. Integração nativa com Email Gateway de mesmo fabricante;

7.9.3.1.5. Integração nativa com *Next Generation Firewal* de mesmo fabricante;

7.9.3.1.6. Deve ser um ponto único para todos os ativos de proteção citados acima e, em nenhum momento, utilizar-se de mais de um *Appliance* para integração e funcionamento aos mesmos.

7.9.4. Detecção de Ameaças

7.9.4.1. Suporta mecanismo de detecção de ameaças (*malwares*) em múltiplas camadas, com no mínimo as seguintes tecnologias de análise:

7.9.4.1.1. Estática – Primeira etapa que determina se um arquivo é uma ameaça (*malware*) conhecida no menor tempo possível, através de:

7.9.4.1.1.1. "Utilização de uma lista local de arquivos confiáveis (lista branca), os quais não precisaram ser analisados por serem notoriamente confiáveis, possuindo mais de 200.000.000 de entradas (arquivos confiáveis) mantidas pelo fabricante do equipamento."

7.9.4.1.1.2. "Utilização de uma lista com valores "MD5 Hash" de arquivos que sejam ameaças (malwares) conhecidas e armazenado em uma base de dados local (lista negra), podendo acrescentar-se, automaticamente a esta lista, novos arquivos que sejam detectados através de heurística ou através de análise dinâmica – quando a severidade for determinada como média, alta ou muito-alta."

7.9.4.1.1.3. "Utilização de um mecanismo de correlação de ameaças (malwares) globais e uma base de inteligência de comportamento de comunicação – ambos baseados em nuvem e permitindo tanto o uso de reputação de arquivos quanto o uso de reputação de endereços IP – onde o comportamento da comunicação inclui reputação, volume e padrões de tráfego de rede."

7.9.4.1.1.4. "Utilização de um mecanismo de análise comportamental de WEB Sites, códigos em WEB Sites e download de conteúdo

WEB 2.0 em tempo real, capaz de detectar modernos “blended attacks”, sem depender de assinaturas de vírus, tais como: vírus, worms, adware, spyware, riskware, e crimeware .”

7.9.4.1.1.5. “Utilização de mecanismo de assinaturas de vírus (DAT), envolvendo também uma análise através de engenharia reversa.”

7.9.4.1.2. Dinâmica – Segunda etapa que, executada logo após a primeira etapa, determina se o comportamento de um arquivo, dentro de máquinas virtuais seguras (sandboxes), é malicioso e representa uma ameaça (malware), através de:

7.9.4.1.2.1. Listagem de todas as DLLs, e seus respectivos “paths”, que forem chamadas por um arquivo em tempo de execução.

7.9.4.1.2.2. Listagem de operações e atividades de arquivos (criar, abrir, consultar, modificar, copiar, mover, apagar), operações de diretórios (criar, excluir), atributos de arquivos e seus respectivos valores “MD5 Hash”.

7.9.4.1.2.3. Listagem de operações de atividades detalhadas de chaves (key) e sub-chaves (sub-keys) no registros do Microsoft Windows (criar, abrir, excluir, modificar, consultar).

7.9.4.1.2.4. Detalhamento de operações e atividades de processos (criar novo processo, terminar processo, criar novo serviço, injetar códigos em outros processos).

7.9.4.1.2.5. Detalhamento de operações e atividades de rede (consultas de DNS, atividade de TCP Socket, download de arquivos via HTTP).

7.9.4.1.3. Suporta detecção de ameaças (*malwares*) dia-zero (“Zero-Day” ou “0-Day”) sem comprometer a qualidade de serviço para os usuários da rede.

7.9.4.1.4. Suporta no mínimo seis (6) níveis de severidade de ameaças (*malwares*), sendo estes níveis de severidade diretamente proporcional ao incremento da pontuação, isto é, quanto maior a pontuação, maior o nível de severidade.

7.9.4.1.5. Suporta no mínimo sete (7) classificações de ameaça (*malware*), através de um sistema de pontuação de ameaça (*threat score*), tais como:

7.9.4.1.5.1. Persistence, Installation Boot Survival;

7.9.4.1.5.2. Hiding, Camouflage, Stealthness, Detection and Removal Protection;

7.9.4.1.5.3. Security Solution / Mechanism bypass, termination and removal, Anti Debugging, VM Detection;
7.9.4.1.5.4. Spreading;
7.9.4.1.5.5. Exploiting, Shellcode;
7.9.4.1.5.6. Networking;
7.9.4.1.5.7. Data spying, Sniffing, Keylogging, Ebanking Fraud.

7.9.4.1.6. Suporta identificação de ameaças (*malwares*) que utilizem técnicas de "*packing*", tentando passar despercebida, garantindo a análise estática do código original ("*unpacking*").
7.9.4.1.7. Suporta identificação de ameaças (*malwares*) que utilizem códigos latentes ("*latent code*") que não são executados durante análise dinâmica.

7.9.5. Compartilhamento de Informações

7.9.5.1. Deve permitir o recebimento de arquivos para análise a partir dos módulos listados acima.

7.9.5.2. Deve implementar um barramento de comunicação aberto para a troca de informações de ameaça entre os diversos módulos propostos neste Termo de Referência;

7.9.5.3. Através da consulta da reputação, A solução deverá permitir:

7.9.5.3.1. Permitir o arquivo a partir da consulta de reputação do mesmo;
7.9.5.3.2. Identificar e monitorar novos arquivos executados no ambiente, devendo efetuar o rastreamento desde a primeira execução.
7.9.5.3.3. Bloqueio do executável uma vez que este for detectado, devendo ser considerado arquivo do tipo malicioso ou suspeito.

7.9.5.4. Deve permitir ao administrador importar reputações de arquivos conhecidos;
7.9.5.5. A reputação deve ser determinada a partir da tentativa de execução em um sistema gerenciado;

7.9.5.6. Deve manter uma base local de reputação já conhecida;

7.9.5.6.1. Para o caso da não existência, o *hash* deverá ser consultado no centro de inteligência do fabricante;

7.9.5.6.2. Para o caso da não existência no centro de inteligência, o mesmo deverá ser encaminhado para análise na solução de ameaças avançadas;

7.9.5.7. Deve apresentar na console central de gestão as seguintes informações:

7.9.5.7.1. Sumário de Eventos dos últimos 30 dias;
7.9.5.7.2. Top 10 Eventos gerados;
7.9.5.7.3. Nome do Certificado;
7.9.5.7.4. Hash do arquivo;
7.9.5.7.5. Regra;
7.9.5.7.6. Sumário do Sistema.

7.10. SERVIÇO DE MONITORAMENTO E PROTEÇÃO DE BASE DE DADOS

7.10.1. Características Gerais

7.10.1.1. Deve prover proteção a dados sensíveis gravados em bases de dados da infraestrutura de TI do BANPARÁ.

7.10.1.2. A solução deve prover os seguintes recursos de forma automatizada:

7.10.1.2.1. Varrer a rede e descobrir banco de dados na rede;
7.10.1.2.2. Proteger os bancos de dados descobertos com um conjunto de defesas pré-configuradas;

7.10.1.3. Prover capacidade de *patching* virtual e proteção completa contra *exploits* conhecidos antes que a correção seja aplicada;

7.10.1.4. Ajudar a criação de uma política de segurança customizada para o ambiente de banco de dados, tornando mais fácil a demonstração de *compliance* a auditores e assim prover proteção aos ativos críticos;

7.10.1.5. Proteger os dados de todas as ameaças, monitorando a atividade local em cada servidor de banco de dados;

7.10.1.6. Alertar ou parar comportamentos maliciosos em tempo real, mesmo quando estiver sendo executado em ambientes virtualizado ou de nuvem de computadores;

7.10.1.7. Prover proteção de banco de dados compatível com padrões internacionais de segurança;

7.10.1.8. Prover solução compatível com pelo menos os seguintes SGBD: ORACLE, MS SQL e MY SQL.

7.10.1.9. Prover console de gerenciamento unificada a solução de gerencia de Endpoint.

7.10.2. Características de escaneamento de vulnerabilidades das bases de dados

7.10.2.1. Prover escaneamento de vulnerabilidades sem a necessidade de instalação de agente *(agent-less*).

7.10.2.2. Prover uma base de dados de pelo menos 4.500 (Quatro mil e quinhentas) checagens, divididas em pelo menos essas categorias:

7.10.2.2.1. Falta de Patches
7.10.2.2.2. Vulnerabilidades conhecidas;
7.10.2.2.3. Código malicioso;
7.10.2.2.4. Backdoors;
7.10.2.2.5. Senhas fracas;
7.10.2.2.6. Dados sensíveis;
7.10.2.2.7. Configurações erradas;
7.10.2.2.8. Código com falhas;
7.10.2.2.9. Falta de conformidade.

7.10.2.3. Ter suporte ao escaneamento nos seguintes SGBDs e versões mínimas:

7.10.2.3.1. Oracle 8i e mais atual;
7.10.2.3.2. Microsoft SQL Server 2000 e mais atual;
7.10.2.3.3. Microsoft SQL Azure;
7.10.2.3.4. IBM DB2 8.1 e mais atual para Linux, Unix e Windows;
7.10.2.3.5. MySQL version 4.0 e mais atual;
7.10.2.3.6. PostgreSQL version 8.3 e mais atual;
7.10.2.3.7. Sybase ASE version 12.5 e mais atual.

7.10.3. Característica de monitoração de atividades dos bancos de dados

7.10.3.1. Proteger base de dados na atual infraestrutura de TI do BANCO, mesmo se estiverem alocadas em ambiente virtualizado ou em ambiente de nuvem computacional;

7.10.3.2. A solução precisa ser em software do tipo sensor-based (não em Appliance);

7.10.3.3. A solução deve ser executada na memória sem qualquer alteração ao kernel do sistema operacional, nem a engine dos SGBDs;

7.10.3.4. O agente não poderá possuir qualquer funcionalidade dependente de outro *Appliance* ou de servidor de gerenciamento;

7.10.3.5. O sensor deve suportar os seguintes SGBDs nas seguintes versões mínimas:

7.10.3.5.1. Oracle version 8.1.7 ou mais atual, sendo executado em Sun Solaris, IBM AIX, Linux, HP-UXe Microsoft Windows;
7.10.3.5.2. Teradata 12, 13, 13.10 and 14 sendo executado em Linux;
7.10.3.5.3. MySQL 5.1, 5.5 e 5.6 sendo executado em Linux;
7.10.3.5.4. Microsoft SQL 2000 e mais atual em qualquer plataforma Windows suportada;
7.10.3.5.5. Sybase ASE 12.5 ou mais atual em todas as plataformas suportadas;
7.10.3.5.6. IBM DB2 LUW 9.5 e 9.7;
7.10.3.5.7. IBM DB2 para Z/OS; e
7.10.3.5.8. IBM DB2 para iSeries (AS/400).

7.10.3.6. A implantação deve ser não intrusiva e consumir o mínimo de recursos, consumir até 150MB de RAM e 5% de processamento;

7.10.3.7. A instalação/desinstalação do agente deve ser realizada sem a necessidade de reinicialização do sistema operacional;

7.10.3.8. Possuir capacidade de aplicar patches e correções de configuração achadas pela varredura de vulnerabilidades e aumentar a postura de segurança das bases de dados imediatamente, sem causar paradas no sistema de banco de dados;

7.10.3.9. Prover proteção completa às ameaças, inclusive de ataques do dia zero, cobrindo base de dados com vulnerabilidades conhecidas mas ainda sem patches, por bloqueio destas vulnerabilidades e finalizando sessões que violam as políticas de segurança;

7.10.3.10. Proteger de todos os vetores de ameaças:

7.10.3.10.1. Local;
7.10.3.10.2. Originada por NW;
7.10.3.10.3. Clear text; ou
7.10.3.10.4. Encriptada.

7.10.3.11. Possuir monitoramento do tráfego local:

7.10.3.11.1. Table views;
7.10.3.11.2. Stored procedures;
7.10.3.11.3. Intra-Hypervisor.

7.10.3.12. Possuir monitoramento e prevenção de tráfego encriptado de banco de dados e SQL Statements ofuscadas;

7.10.3.13. Possuir monitoramento e prevenção de atividades indesejadas mesmo sendo realizadas por usuários privilegiados;

7.10.3.14. Possuir monitoramento e prevenção de conexões indesejadas a base de dados;

7.10.3.15. Possuir monitoramento e prevenção de acesso a dados sensíveis;

7.10.3.16. Possuir monitoramento e prevenção de acessos no nível dos componentes (*Facilitate monitoring & prevention of access down to database component level*.);

7.10.3.17. Possuir relatórios flexíveis, incluindo modelos de relatórios pré-configurados e customizáveis;

7.10.3.18. Prover relatórios de trilhas de auditoria detalhados adequando-se aos padrões de segurança, ajudando o BANCO em uma análise forense pós-incidente a entender a quantidade de informação perdida e atividades maliciosas;

7.10.4. Características de gerenciamento da solução

7.10.4.1. A Solução de Monitoramento e Proteção de Base de Dados devem ser gerenciados a partir de console única e que seja a mesma console de gerência de *endpoint*.

7.10.4.2. A console deve gerenciar além da solução proposta as seguintes tecnologias:

7.10.4.2.1. Solução de Proteção das Estações de Trabalho e Servidores de Rede;
7.10.4.2.2. Solução de Proteção Contra Vazamento e Integridade dos Dados;

7.10.4.3. A console de gerenciamento de segurança deve ser baseada em WEB, prover regras de acesso granulares e facilitar a trilha de auditoria administrativa;

7.10.4.4. Deve prover profunda capacidade de gerenciamento de ativos com suporte a:

7.10.4.4.1. *Tagging*;
7.10.4.4.2. Ações automatizados baseadas nas tags.
7.10.4.4.3. Deve prover nativamente biblioteca de *dashboards* com capacidade de drill down;
7.10.4.4.4. Deve prover nativamente biblioteca de queries e relatórios que possam ser customizados facilmente;
7.10.4.4.5. Deve prover acesso rápido a adição e customização de *dashboards*;

7.10.4.5. Deve suportar extensibilidade para:

7.10.4.5.1. Adição de varredura sem necessidade de agentes (*agent-less*) para todos os componentes da infraestrutura de TI, usando FASL-scripts;
7.10.4.5.2. Adição de varredura sem necessidade de agentes (*agent-less*) em aplicações WEB;
7.10.4.5.3. Adição de política baseada em agente para:
7.10.4.5.4. OVAL-checks;

7.10.4.6. Possuir capacidade de extensão para Risk Management nativamente;

7.10.4.7. Possuir capacidade de receber *feeds* de centros de pesquisas a ameaças e realizar correlação de risco entre as últimas ameaças e os ativos atuais e suas vulnerabilidades;

7.10.4.8. Deve prover interação a diversos fornecedores e terceiros, permitindo integração via APIs.

8. PRAZOS DE EXECUÇÃO E DE ACEITE E NATUREZA DOS SERVIÇOS

Os serviços de que tratam os itens 1 a 9 referem-se à prestação de serviços mensais, de natureza contínua, razão pela qual podem vigorar pelo período de até 60 meses, tendo como fundamento o que dispõe o inc. II, art. 57 da Lei nº 8.666/93. O período de prestação, a partir da emissão do termo de recebimento definitivo, será o estabelecido na tabela abaixo, observadas as etapas previstas de planejamento, customização de ambiente e instalação de ativos de rede, deste Termo.

Item	Descrição	Quantidade	Meses
1	Serviço de Firewall Próxima Geração e VPN	1	48
2	Serviço de Prevenção de Intrusos	1	48
3	Serviço de Gestão de Risco e Compliance	1	48
4	Serviço de Gateways de Email e Web	1	48
5	Serviços de Proteção das Estações de Trabalho e Servidores de Rede	1	48
6	Serviço de Proteção Contra Vazamento e Integridade dos Dados	1	48
7	Serviço de Gestão de Eventos e Incidentes	1	48
8	Serviço de Proteção Contra Ameaças Dia Zero	1	48
9	Serviço de Monitoramento e Proteção de Base de Dados	1	48

8.1. O item 10 refere-se à prestação de serviços de treinamento que deverão ser solicitados por meio de Ordem de Serviço de Treinamento (Anexo III) cuja execução deve ser recebida por meio do Termo de Recebimento de Serviços de Treinamento (Anexo IV). Tais serviços deverão ser prestados em, no máximo, 4 (quatro) meses após o recebimento definitivo dos serviços alvo do treinamento.

8.2. O item 12 refere-se à prestação de serviços técnicos especializados de natureza eventual, sendo demandados de acordo com as necessidades do BANPARÁ, solicitados por meio de Ordem de Serviço (Anexo V) cuja execução deve ser recebida por meio do Termo de Recebimento de Serviços (Anexo IV).

8.3. A partir da assinatura do contrato, correrão os seguintes prazos:

8.3.1. Reunião de início do projeto (kick-off): 10 (dez) dias corridos;

8.3.2. Entrega do Projeto Executivo: 40 (quarenta) dias corridos;

8.3.2.1. O BANPARÁ se manifestará no prazo de 10 (dez) dias corridos, contados da data de entrega do Projeto Executivo;

8.3.2.2. Havendo necessidade de ajustes, a contratada terá 10 (dez) dias corridos para realizá-los, contados da notificação a ser efetuada pelo BANPARÁ, a respeito da manifestação sobre o Projeto Executivo;

9. VISITA TÉCNICA

9.2. Para que a empresa licitante compreenda a complexidade do ambiente tecnológico do BANPARÁ, haverá a realização de visita técnica até 4 (quatro) dias úteis antes da data de abertura das propostas, que terá seu respectivo atestado emitido após sua realização;

9.3. A Visita técnica deverá ser realizada por um representante legal da empresa LICITANTE ou por seu procurador, devidamente autorizado através de procuração;

9.4. A comprovação deverá ser através de uma declaração emitida pelo próprio licitante (modelo no anexo I) de que está de acordo com a realização dos serviços, não tendo nenhuma dúvida que venha a modificar ou prejudicar os quantitativos e especificações indicadas no Termo de Referência.

10. COMPROVAÇÕES – APRESENTAR COM A PROPOSTA DE PREÇOS

10.2. Os documentos exigidos neste procedimento licitatório poderão ser apresentados em original, por meio de fotocópias autenticadas por cartório competente ou servidor da

administração, ou fotocópias simples (exceto cópia de FAX) acompanhadas dos originais para cotejo no ato da apresentação.

10.3. Para fins de habilitação serão exigidas as seguintes comprovações técnicas:

10.3.2. Declaração de atendimento da LICITANTE aos requisitos de Infraestrutura dos centros de operações de segurança (SOC) especificados no item 3.1 deste documento, disponibilizando o ambiente para auditoria por parte do BANPARÁ;

10.3.3. Certificados em nome dos profissionais para fins de comprovação do item 3.2.5 deste termo de referência, cópias dos documentos exigidos no item 3.2.6 referente ao vínculo destes profissionais;

10.3.4. Declarações conferidas por empresas públicas ou privadas, para fins de comprovação do item 3.3.1 deste termo de referência;

10.3.5. Declaração dos fabricantes das soluções, para fins de comprovação do item 3.3.2 deste termo de referência;

10.3.6. Atestado de Visita Técnica, para fins de comprovação do item 7 (VISITA TÉCNICA) deste termo de referência.

11. REQUISITOS OBRIGATÓRIOS GERAIS

11.2. A documentação exigida neste item deverá ser como anexo à **PROPOSTA DE PREÇOS**;

11.3. Todas as características técnicas exigidas na especificação das soluções técnicas deverão ser comprovadas, independente da descrição da proposta, através de documentos cujas origens sejam exclusivamente o fabricante dos equipamentos, como catálogos, manuais, ficha de especificação técnica ou páginas obtidas no site oficial dos fabricantes, sob a forma de volumes impressos ou em meio eletrônico (CD, DVD, etc.);

11.4. As informações obtidas em sites oficiais do fabricante através da Internet deverão ser impressas e anexadas à proposta e deverá ser indicado à respectiva URL (*Uniform Resource Locator*) onde se encontram;

11.5. Serão aceitos documentos em português ou inglês para comprovações técnicas;

11.6. A equipe técnica do BANPARÁ poderá realizar pesquisas adicionais para corroborar o atendimento, ou não, das características técnicas exigidas na especificação das soluções técnicas, caso a documentação apresentada seja insuficiente ou deixe dúvidas;

11.7. A não comprovação de alguma característica exigida levará a desclassificação da proponente.

12. CONDIÇÕES DE ENTREGA E IMPLANTAÇÃO DOS SERVIÇOS

12.2. O prazo para entrega dos equipamentos e sistemas que compõem o serviço pela CONTRATADA será de 60 (sessenta) dias consecutivos, contados a partir da data da assinatura do contrato;

12.3. Os equipamentos e sistemas que compõem o serviço deverão ser entregues e instalados no BANPARÁ. As fases da implantação do serviço devem contemplar:

12.4.1. Planejamento: nesta etapa a CONTRATADA deverá realizar o planejamento do projeto, onde serão definidos os prazos por atividade, as pessoas, a estratégia de implantação do serviço, o plano testes, a localização dos Appliances na arquitetura da rede do BANPARÁ, bem como quaisquer outros itens que sejam necessários para a implantação do projeto. Devem-se considerar as janelas de manutenção do BANPARÁ, plano de rollback e o escopo definido. Os responsáveis técnicos do BANPARÁ acompanham e aprovam o planejamento.

12.4.1.1. Os prazos para a implantação de cada um dos serviços, pela CONTRATADA, estão especificados na tabela 13. O prazo passa a ser contado a partir da data acordada entre o BANPARÁ e a CONTRATADA para implantação do serviço, com aceite oficial do BANPARÁ, após a data de recebimento dos equipamentos no BANPARÁ:

Serviço	**Tempo Máximo de Implantação (Dias Corridos)**
Firewall Próxima Geração e VPN	90
Prevenção de Intrusos	90
Gestão de Risco e Compliance	60
Gateway de E-mail e Web	60
Proteção das Estações de Trabalho e	60

Servidores de Rede	
Proteção Contra Vazamento e Integridade dos Dados	120
Gestão de Eventos e Incidentes	90
Proteção Contra Ameaças Dia Zero	90
Monitoramento e Proteção de Base de Dados	60

Tabela 13: Prazo para implantação dos serviços por categoria.

12.4.2. Implementações: após a aprovação do planejamento deverá ser iniciado o processo de implantação, levando-se em consideração a disponibilidade das equipes envolvidas, cumprimento dos prazos pactuados e o foco principal do projeto: tornar o ambiente mais seguro e controlado, quanto à confidencialidade, integridade e disponibilidade do ambiente.

12.4.3. Etapa de testes: todos os controles implantados para a ativação dos serviços gerenciados de segurança deverão ser testados a cada etapa pré-definida no planejamento. Além disso, o plano de rollback deverá garantir o retorno exequível e ágil, caso ocorra alguma falha no processo de implantação dos controles necessários à prestação do serviço.

12.4.4. Homologação: Após a conclusão dos testes, a solução deverá ser formalmente homologada pelo BANPARÁ, com a finalidade de iniciar a monitoração, operação dos serviços e gerenciamento do ambiente, dentro do NMS acordado.

12.4.4.1. O BANPARÁ terá o prazo de 15 (quinze) dias consecutivos, contados a partir da data de conclusão dos serviços de instalação e configuração do(s) serviços contratados, para emitir o relatório de homologação (aceite);

12.4.4.2. O(s) serviço(s) será (ão) aceito(s) se e somente se houver comprovação de que todos os requisitos técnicos especificados neste Termo de Referência tenham sido atendidos. Essa comprovação será feita mediante observação direta das características dos equipamentos, consulta à documentação técnica fornecida e verificação dos serviços de instalação e configurações, comparadas aos termos deste edital;

12.4.5. Documentação: A CONTRATADA deverá elaborar e manter atualizada documentação das atividades e de todos os processos.

12.4.5.1. Devem ser documentados: entrega e conferência, testes, homologação, compromissos e prazos, incluindo planos de trabalho, planos de contingência, cronogramas, atas de reuniões, de modo a compor documentação (“as built”) a ser entregue o BANPARÁ ao final da implantação. Ao BANPARÁ poderá propor atualizações nesse documento, no sentido de melhor atender ao bom andamento dos trabalhos ou à própria conveniência do BANPARÁ.

12.4.5.2. Com a finalização da etapa de testes e homologação deverá ser realizada uma apresentação in-loco, com a finalidade de registrar as intervenções realizadas no ambiente ativo atual, apresentar a metodologia do serviço gerenciado ao BANPARÁ, formalizar o Plano de Comunicação, formatar a Matriz de Responsabilidades (com os nomes e pessoas-chave responsáveis) e ratificar o SLA da solução contratada.

13. VALOR DO SERVIÇO

13.1. A tarifação do serviço compreenderá os seguintes valores, a serem expressos em R$ (reais):

13.1.1. Taxa de Instalação para cada um dos serviços, cobrada uma única vez, incluindo o planejamento, implementação e teste de todas as funcionalidades contratadas. Este valor não poderá ultrapassar 20% do valor total do contrato;

13.1.2. Assinatura Mensal, incluindo o direito de uso dos serviços, em comodato dos equipamentos, em regime 24x7x365 (vinte e quatro horas por dia, sete dias por semana, 365 dias por ano), todos os dias do ano, considerando um contrato de 48 meses;

13.1.3. Disponibilização de um banco de horas, a ser utilizado sob demanda;

13.1.4. Valor total para treinamento de todos os serviços especificados neste Termo.

13.2. O Total geral do contrato, para 48 meses, será o valor a ser utilizado como base para os lances do pregão. Este valor será composto pela soma das taxas de instalação de todos os serviços, pela soma das mensalidades de todos os serviços considerando 48 meses, do valor total do banco de horas, o valor total cobrado pelos treinamentos de todos os serviços.

13.3. Os preços ofertados em lance licitatório obrigarão a licitante a manter, a mesma relação proporcional inicial, entre todos os itens de cobrança que compõem a planilha de preços.

14. DO PAGAMENTO

14.1. Os pagamentos a serem realizados serão efetuados da seguinte forma:

14.1.1. Cada uma das inicializações das implantações das soluções terá parcela única cobrada referente a ela, sendo que poderão ser pagas em até 30 dias após a apresentação do termo de aceite pelo BANPARÁ para inicialização das implantações;

14.1.2. O termo de aceite só será emitido perante comprovação do perfeito funcionamento da ferramenta implantada.

14.1.3. A inicialização da implantação de cada uma das soluções deverá ser comprovada pela CONTRATADA, através de testes efetuados pela sua Área de Segurança.

14.1.4. Os treinamentos especificados no item TREINAMENTOS, da planilha de preços (ANEXO II do edital), serão pago após a realização de todos os itens (01 a 12), em parcela única, paga em até 30 dias após a emissão do respectivo termo de aceite referente ao último treinamento efetuado.

14.1.5. Parcela fixa mensal pela prestação dos serviços de manutenção e suporte técnico da solução, a ser paga até o décimo dia do mês subsequente da prestação do serviço, estando o pagamento da primeira parcela condicionada ao aceite da realização do treinamento, sendo que a cobrança deste serviço somente poderá ser iniciada após a implantação da solução.

14.1.6. Qualquer objeto de cobrança terá que ter sido previamente homologado e/ou conferido, assim, para que o respectivo pagamento se efetive deverá a Nota Fiscal/Fatura ser apresentada ao Banco com antecedência mínima de 30 dias do vencimento, ficando este isento de responsabilidade por atrasos na apresentação das faturas por parte da CONTRATADA.

14.1.7. Nenhum pagamento será efetivado sem que representantes do Banco atestem, por meio de Termo de Aceite e/ou Termo de Homologação, que o objeto contratado está integralmente sendo entregue/disponibilizado e/ou cumprido pela CONTRATADA.

14.1.8. A realização de qualquer pagamento pelo Banco fica condicionada a apresentação dos seguintes documentos: CND- emitida pelo INSS, Certidão de Regularidade da Receita Federal e da PGFN, CND do FGTS expedida pela CEF; prova de regularidade para com as fazendas Estadual e Municipal do domicílio da sede da CONTRATADA.

14.1.9. A devolução da Nota/Fatura não servirá de pretexto ao descumprimento de quaisquer das obrigações da CONTRATADA.

14.1.10. O Banco efetuará o pagamento via crédito em conta corrente a ser aberta pela CONTRATADA em uma das agências do Banco do Estado do Pará S/A - BANPARÁ, a qual deverá ser indicada na nota fiscal/fatura, conforme dispõe o Decreto do Estado do Pará nº 877/2008.

14.1.11. Nenhum pagamento será efetuado à CONTRATADA, enquanto pendente de liquidação qualquer obrigação financeira que lhe for imposta em virtude de penalidade ou inadimplência contratual.

14.1.12. Sem prejuízo ao pagamento das multas estipuladas no contrato, o Banco poderá suspender quaisquer pagamentos devidos à CONTRATADA, sem incorrer em ônus adicionais, sempre que sua área gestora do contrato constatar a ocorrência de atrasos na execução do objeto contratado, retomando-os tão logo tais atrasos sejam completamente eliminados nos termos de parecer da área gestora do contrato.

14.1.13. Todo e qualquer prejuízo ou responsabilidade, inclusive perante o Judiciário, e órgãos administrativos, atribuídos ao Banco, oriunda de problemas na execução do contrato por parte da CONTRATADA, serão repassadas a esta e deduzidas do pagamento realizado pelo Banco, independente de comunicação ou interpelação judicial ou extrajudicial.

14.1.14. No preço apresentado pela CONTRATADA já estão incluídos todos os tributos e demais encargos que incidam ou venham a incidir sobre o contrato, assim como contribuições previdenciárias, fiscais e parafiscais, PIS/PASEP, FGTS, IRRF, emolumentos, seguro de acidente de trabalho, e outros, ficando excluída qualquer solidariedade do Banco, por eventuais autuações.

14.1.15. De acordo com a legislação tributária e fiscal em vigor, será efetuada a retenção na fonte dos tributos e contribuições incidentes no objeto contratado.

15. PENALIDADES

15.1. Em caso da não implementação dos serviços no prazo previsto, sem justificativas aceitas pelo BANPARÁ, serão aplicadas as seguintes penalidades:

15.1.1. Desconto de 0,25% (zero vírgula vinte e cinco por cento) do valor global do contrato, por dia de atraso na conclusão da implantação da solução, dedutível do valor da fatura de implantação (13.1.1), limitados a 30 dias;

15.1.1.1. Após o 30º (trigésimo) dia de atraso, e a critério do BANPARÁ, poderá ocorrer a não aceitação do objeto, de forma a configurar, nessa hipótese, inexecução total da obrigação assumida, sem prejuízo da rescisão unilateral da avença.

15.1.2. Multa de 10% do valor global do contrato, no caso de inexecução parcial da obrigação, sem prejuízo de aplicação de outras penalidades;

15.1.3. Multa de 15% do valor global do contrato, no caso de inexecução total da obrigação, sem prejuízo de aplicação de outras penalidades;

15.1.4. Multa de 30% do valor global do contrato, no caso de rescisão por culpa da contratada, sem prejuízo de aplicação de outras penalidades;

15.2. Caso o percentual de atendimento seja inferior a 95% por três meses consecutivos do NMS especificado, será aplicada multa no valor de 1% (um por cento) do valor global do contrato.

16. OBRIGAÇÕES E RESPONSABILIDADES DA CONTRATADA

16.1. Assegurar-se que o local de instalação dos equipamentos necessários à prestação dos serviços possui as condições técnicas e ambientas necessárias ao funcionamento dos equipamentos necessários aos serviços;

16.2. Manter Centros de Operação de Segurança (SOC) próprios para monitoramento remoto 24x7x365, com infraestrutura estritamente de acordo com as especificações deste documento;

16.3. Implantar todos os softwares e hardwares necessários à prestação dos serviços de monitoração, gerência e administração remota da segurança, conforme as especificações técnicas constantes deste Termo de Referência;

16.4. A CONTRATADA será responsável pela manutenção preventiva e corretiva dos hardwares e softwares por ela ofertados;

16.5. Todas as soluções de hardware e Software, ambientes de gerenciamento e monitoramento devem ser fornecidos em regime de comodato;

16.6. Iniciar a prestação dos serviços dentro dos prazos estabelecidos neste Termo de Referência;

16.7. Implementar/gerenciar backup de configuração de sistemas gerenciados;

16.8. Realizar qualquer alteração na configuração da solução (aplicação de novas regras, exclusão de regras, atualização de versões, aplicações de "patches", etc.) mediante autorização do BANPARÁ;

16.9. Comunicar, imediatamente, a eminência ou ocorrência de incidentes de segurança: os acessos indevidos, instalação de códigos maliciosos, indisponibilização dos serviços (DoS), ataques por força bruta, ou qualquer outra ação que vise prejudicar a funcionalidade dos serviços do BANPARÁ;

16.10. As implantações das soluções serão realizadas pela CONTRATADA e todas as atividades envolvidas serão acompanhadas e coordenadas por analistas e técnicos do BANPARÁ;

16.11. Resolver os chamados de serviço e suporte técnico conforme os tempos definidos nas tabelas de tempos de atendimento (SLA) deste Termo de Referência;

16.12. Substituir equipamentos com defeito, que cause a indisponibilidade de serviço dependente do mesmo, conforme o tempo estipulado na tabela de tempos de atendimento (SLA);

16.13. Manter os serviços contratados nos níveis de disponibilidade estabelecidos em item específico deste Termo de Referência;

16.14. A implantação das soluções, quando realizadas no ambiente de produção, poderão ter as atividades executadas após o expediente (horários noturnos ou em finais de semana e feriados);

16.15. A CONTRATADA será responsável por efetuar as atividades de integração da solução de monitoração remota com o ambiente operacional do BANPARÁ, sem prejuízo aos serviços desta;

16.16. Quando previamente acordado entre as partes, a CONTRATADA poderá realizar serviços de monitoramento in loco com o acompanhamento de um representante do BANPARÁ.

16.17. Registrar os tempos de atendimento dos chamados de suporte técnico ou chamados de serviços, mensais e anuais, indicando os chamados que foram atendidos dentro e fora do SLA estabelecido neste termo de referência;

16.18. Produzir e enviar por e-mail, mensalmente, relatórios analíticos a equipe gestora do BANPARÁ, ou em 24h quando for demandado;

16.19. Participar, mensalmente, de reuniões presenciais, de ponto de controle, para apresentação dos indicadores de disponibilidade, diagnósticos dos ambientes monitorados, dirimir dúvidas sobre o serviço contratado, análise e entendimento dos relatórios gerenciais e administrativos, revisão das configurações e procedimentos implementados e melhorias a serem implementadas;

16.20. Garantir e manter total e absoluto sigilo sobre as informações manuseadas, as quais devem ser utilizadas apenas para a condução das atividades autorizadas, não podendo ter quaisquer outros usos, sob pena de rescisão contratual e medidas cíveis e penais cabíveis, assumindo inteira responsabilidade pelo uso indevido ou ilegal de informações privilegiadas do BANPARÁ, praticado por seus empregados, conforme Acordo de Responsabilidade para Fornecedores, a ser assinado pela CONTRATADA no ato da assinatura do contrato.

17. OBRIGAÇÕES E RESPONSABILIDADES DA CONTRATANTE

17.1. Providenciar as condições técnicas e ambientais necessárias à implantação e funcionamento dos serviços;

17.2. Providenciar as autorizações de acesso aos técnicos da CONTRATADA, desde que devidamente agendado e os técnicos identificados, aos locais de instalação das soluções para as implantações e nos casos de manutenções;

17.3. Informar aos técnicos da CONTRATADA as necessidades de configuração dos equipamentos e serviços. Estas informações serão repassadas para a CONTRATADA através da abertura de chamados de suporte técnico. Quando necessário, podem ser anexados aos chamados arquivos com as necessidades de configurações;

17.4. Cumprir pontualmente todos os seus compromissos financeiros para com a CONTRATADA;

17.5. Proporcionar todas as facilidades para que a CONTRATADA possa executar os serviços de que trata este Termo de Referência, dentro das normas e condições estabelecidas em contrato;

17.6. Comunicar à CONTRATADA todas as possíveis irregularidades detectadas na execução dos serviços contratados, para a pronta correção das irregularidades apontadas;

17.7. Fiscalizar diretamente a execução dos serviços de que trata o objeto deste Termo de Referência, atestando a sua prestação se, e somente se, os serviços executados atenderem plenamente às especificações constantes deste Termo de Referência.

17.8. Rejeitar, no todo ou em parte, a solução entregue pela CONTRATADA fora das especificações deste Termo de Referência.

17.9. A fiscalização de que trata este item não exclui nem reduz a responsabilidade da CONTRATADA pelos danos causados ao BANPARÁ ou a terceiros, resultantes de ação ou omissão culposa ou dolosa de quaisquer de seus empregados ou prepostos.

DECLARAÇÃO DE VISITA TÉCNICA

A empresa ....., inscrita no CNPJ sob o nº .....DECLARA, para fins de habilitação no procedimento licitatório, exigência do item 12.1.4, do PREGÃO ELETRÔNICO nº...../2011, que nesta data, preposto seu, abaixo assinado, compareceu às instalações do BANCO DO ESTADO DO PARÁ, situado no endereço localizado, na Rua Municipalidade Nº 1036 – Bairro: Umarizal, CEP: 66050350, e na Matriz localizado na Av. Pte. Vargas Nº 251, Bairro: Centro, CEP: 66010000, onde foi perfeitamente cientificado das peculiaridades, do padrão e da complexidade dos serviços a serem executados, de acordo com o objeto da licitação.

Belém-Pará.....de.....2011

.....

Assinatura do Vistoriador

Nome:

RG/Matrícula.

Cargo/Função que exerce na empresa:

Visto/Carimbo

(Pelo BANCO DO ESTADO DO PARÁ)

.....

ANEXO II – MODELO DE PREÇOS

PREGÃO ELETRÔNICO Nº /2015 - BANCO DO ESTADO DO PARÁ S/A

Ao Banco do Estado do Pará
À Pregoeira
Processo Nº 1708/2015 – BANPARA/SUSEM/GESEI – Edital nº /2015.

Apresentamos a V.S.ª, nossa proposta de preços para a Contratação de empresa especializada, para Fornecimento de Solução Integrada de Serviços Gerenciados de Segurança compreendendo: provimento de serviços de proteção de perímetro interno e externo; monitoramento e administração dos serviços providos; gestão de conformidade e padrões; resposta a incidentes de segurança e transferência de conhecimento para o corpo técnico do BANPARÁ, conforme especificações técnicas, condições e exigências estabelecidas no termo de referência contemplando:

LOTE				
ITEM	**DESCRIÇÃO**	**QTD**	**PREÇO UNITÁRIO**	**TOTAL 48 MESES (R$)**
1	Serviço de Firewall Próxima Geração e VPN, fornecido com no mínimo 2 appliances em cluster ativo/ativo e um appliance de gerência (este de gerência podendo ser uma máquina virtual);	**48**		
1.1	Inicialização dos Serviços da Solução de Firewall Próxima Geração e VPN	**1**		
2	Serviço de Prevenção de Intrusos, fornecido com no mínimo 5 appliances, sendo 2 appliances em cluster ativo/failover para proteção da borda e 2 appliances em cluster ativo/failover para proteção da rede interna e 1 (um) appliance de gerência;	**48**		
2.1	Inicialização do Serviço de Prevenção de Intrusos	**1**		
3	Serviço de Gestão de Risco e Compliance fornecido com no mínimo 2 appliances, com capacidade e licenciamento para 2800 endereços IP;	**48**		
3.1	Inicialização do Serviço de Gestão de	**1**		

	Risco e Compliance			
4	Serviço de Gateways de Email e Web fornecido com no mínimo 4 (quatro) appliances 2 (dois) em cluster ativo/ativo para o serviço de gateway de email e 2 (dois) appliances em cluster ativo/ativo para o serviço de gateway de web, licenciados para no mínimo 2000 usuários.	**48**		
4.1	Inicialização do Serviço de Gateways Email e Web	**1**		
5	Serviços de Proteção das Estações de Trabalho e Servidores de Rede fornecido com software licenciado para 2800 (dois mil e oitocentos) hosts;	**48**		
5.1	Inicialização dos Serviços de Proteção das Estações de Trabalho e Servidores de Rede	**1**		
6	Serviço de Proteção Contra Vazamento e Integridade dos Dados fornecido com no mínimo 3 appliances e software licenciado para 2800 (dois mil e quinhentos) hosts;	**48**		
6.1	Inicialização dos Serviços de Proteção contra vazamento e integridade dos dados.	**1**		
7	Serviço de Gestão de Eventos e Incidentes fornecido com no mínimo 1 (um) appliance;	**48**		
7.1	Inicialização do Serviço de Gestão de Eventos e Incidentes	**1**		
8	Serviço de Proteção Contra Ameaças Dia Zero fornecido com no mínimo 2 appliances em cluster ativo/ativo;	**48**		
8.1	Inicialização do Serviço de Proteção Contra Ameaças Dia Zero	**1**		
9	Serviço de Monitoramento e Proteção de Base de Dados	**48**		
9.1	Inicialização do Serviço de Monitoramento e Proteção de Base de Dados	**1**		
10	**TREINAMENTOS**			
10.1	Treinamento Firewall Próxima Geração e VPN	**1**		
10.3	Treinamento Gestão de Risco e Compliance	**1**		
10.4	Treinamento Gateway de Email e Web	**1**		

10.5	Treinamento Proteção das Estações de Trabalho e Servidores	**1**		
10.6	Treinamento Proteção contra Vazamento e Integridade dos Dados	**1**		
10.7	Treinamento Gestão de Eventos e Incidentes	**1**		
10.8	Treinamento Proteção Contra Ameaças Dia Zero	**1**		
10.9	Treinamento Monitoramento e Proteção de Base de Dados	**1**		
11	Monitoração e Administração de Segurança	**1**		
12	Serviços Técnicos Especializados	**1**		
TOTAL GLOBAL				

O prazo de validade da proposta de preços é de **120 (cento e vinte) dias consecutivos**, contados da data da abertura da licitação.

Prazo de Vigência do Contrato de 48 (Quarenta e oito) meses, contados a partir de sua assinatura.

Declaramos que o(s) objeto(s) serão entregue(s) estritamente de acordo com as especificações, condições, exigências constantes do Termo de Referência Anexo I do edital, bem como, nos seus demais anexos, sob pena de não serem aceitos pelo órgão licitante.

Declaramos que estamos de pleno acordo com todas as condições e exigências estabelecidas no Edital e seus Anexos, bem como aceitamos todas as obrigações e responsabilidades especificadas no edital, termo de referência e contrato.

Declaramos estar cientes da responsabilidade administrativa, civil e penal, bem como ter tomado conhecimento de todas as informações e condições necessárias à correta cotação do objeto licitado.

Declaro que os preços propostos estão incluídos todos os custos e despesas, inclusive taxas, impostos, tributos, contribuições sociais, parafiscais, comerciais e outros inerentes ao objeto relativo ao procedimento licitatório PREGÃO ELETRÔNICO N. /2015.

Caso nos seja adjudicado o objeto da licitação, comprometemos a assinar o contrato no prazo determinado no documento de convocação, e para esse fim fornecemos os seguintes dados:

ATENÇÃO: Caso não informado abaixo a agência e conta aberta no Banco do Estado do Pará, em cumprimento ao art. 2º do Decreto Estadual n.º 877/2008 de 31/03/2008, o licitante deverá apresentar a seguir declaração:

"**NOS COMPROMETEMOS A REALIZAR A REFERIDA ABERTURA DA CONTA NO PRAZO MÁXIMO DE ATÉ 05 (CINCO DIAS) CONSECUTIVOS CONTADOS DA ASSINATURA DO CONTRATO."**

Razão Social: _____
CNPJ/MF: _____
Endereço: _____
Tel./Fax: _____
Endereço Eletrônico (e-mail):
CEP: _____
Cidade: _____ UF: _____
Banco: 037 Agência: _____ c/c: _____

Dados do Representante Legal da Empresa:
Nome:_____
Endereço:_____
CEP:_____Cidade:_____UF:_____
CPF/MF:_____Cargo/Função:_____
RG nº:_____Expedido por: _____
Naturalidade: _____Nacionalidade: _____

OBSERVAÇÕES:
Em caso de discordância existente entre as especificações deste objeto descritas no COMPRASNET - CATMAT e as especificações constantes do Anexo.1 deste edital, prevalecerão as últimas.

ANEXO II-A - MODELO DE DECLARAÇÃO DE ELABORAÇÃO INDEPENDENTE DE PROPOSTA

Pregão Eletrônico ____/2015

A empresa _____, CNPJ _____, por meio de seu representante legal, para fins do disposto no Edital do Pregão Eletrônico nº ____/2014 UASG 925803, declara, sob as penas da lei, em especial o art. 299 do Código Penal Brasileiro, que:

(a) a proposta apresentada para participar do Pregão Eletrônico ____/2014 UASG 925803 foi elaborada de maneira independente pela empresa _____ e o conteúdo da proposta não foi, no todo ou em parte, direta ou indiretamente, informado, discutido ou recebido de qualquer outro participante potencial ou de fato do Pregão Eletrônico ____/2014 UASG 925803, por qualquer meio ou por qualquer pessoa;

(b) a intenção de apresentar a proposta elaborada para participar do Pregão Eletrônico ____/2014 UASG 925803, não foi informada, discutida ou recebida de qualquer outro participante potencial ou de fato do Pregão Eletrônico ____/2014 UASG 925803, por qualquer meio ou por qualquer pessoa;

(c) que não tentou, por qualquer meio ou por qualquer pessoa, influir na decisão de qualquer outro participante potencial ou de fato do Pregão Eletrônico ____/2014 UASG 925803, quanto a participar ou não da referida licitação;

(d) que o conteúdo da proposta apresentada para participar do Pregão Eletrônico ____/2014 UASG 925803, não será, no todo ou em parte, direta ou indiretamente, comunicado ou discutido com qualquer outro participante potencial ou de fato do Pregão Eletrônico ____/2014 UASG 925803 antes da adjudicação do objeto da referida licitação;

(e) que o conteúdo da proposta apresentada para participar do Pregão Eletrônico ____/2015 UASG 925803 não foi, no todo ou em parte, direta ou indiretamente, informado, discutido ou recebido de qualquer integrante de BANCO DO ESTADO DO PARÁ S/A antes da abertura oficial das propostas; e

(f) que está plenamente ciente do teor e da extensão desta declaração e que detém plenos poderes e informações para firmá-la.

Belém (PA), ____ de _____ de 2015

_____

Nome e Assinatura do Representante Legal da Empresa

ANEXO III – ORDEM DE SERVIÇO DE TREINAMENTO

ORDEM DE SERVIÇO DE TRENAMENTO

Nº: _____

Treinamento:
Considerando:
Especificação do treinamento a ser executado:
Participantes:
_____ _____ **SUSEM/GESEI** **Prestador(a) de serviço(s)** **Data: _____**

1ª via SUSEM/GESEI - 2ª via Prestador de serviços

ANEXO VI – TERMO DE RECEBIMENTO DE SERVIÇOS DE TREINAMENTO

TERMO DE ACEITE DE ATIVIDADE

□ Instalação	**□ Treinamento**	**□ Correção/Alteração - No. Chamado( )**
□ Outra:		
Descrição da Atividade:		
Atividade concluída com sucesso □ SIM □ NÃO		
Data		
Funcionário Banpará	**Matricula**	**Assinatura**
Funcionário Contratada	**Identificação**	**Assinatura**

Observações:

- O material didático mínimo fornecido pela CONTRATADA, para a realização desse treinamento, será uma apostila com todo o conteúdo do curso, em formato digital e impresso, preferencialmente em português;
- Caso a avaliação do curso não seja satisfatória, a CONTRATADA será obrigada a ministrar novo treinamento, sem ônus ao CONTRATANTE.

ANEXO V – ORDEM DE SERVIÇO

ORDEM DE SERVIÇO - Nº: _____

Assunto:
Considerando:
Especificação do Serviço a ser executado:
_____ _____ **SUSEM/GESEI** **Prestador(a) de serviço(s)** **Data: _____**

1ª via SUSEM/GESEI - 2ª via Prestador de serviços

ANEXO VI – TERMO DE CONFIDENCIALIDADE, ZELO E RESPONSABILIDADE

TERMO DE CONFIDENCIALIDADE, ZELO E RESPONSABILIDADE SOBRE OS BENS DE INFORMAÇAO DO BANCO DO ESTADO DO PARA S.A.

CONTRATADO:

Pelo presente termo de confidencialidade, zelo e responsabilidade, considerando que os bens de informação a mim disponibilizados por força de contrato celebrado com o BANPARÁ são de propriedade deste e devem ser utilizados com o único e exclusivo objetivo de permitir a adequada prestação dos serviços contratados e, ciente dos cuidados necessários à preservação e proteção de todos os bens de informação da instituição, inclusive em relação ao dever de sigilo, comprometo-me a:

I. Seguir as diretrizes da política de segurança e proteção dos bens de informação do BANPARÁ, sob pena de responsabilização penal ou civil cabíveis;

II. Utilizar os bens de informação disponibilizados por força de contrato celebrado com o BANPARÁ exclusivamente para fins da adequada prestação dos serviços contratados, estritamente em observância aos interesses do BANPARÁ;

III. Respeitar a propriedade do BANPARÁ ou de terceiros, sobre os bens de informação disponibilizados, zelando pela integridade dos mesmos, não os corrompendo ou os divulgando a pessoas não autorizadas;

IV. Manter, a qualquer tempo e sob as penas de lei, total e absoluto sigilo sobre os bens de informação do BANPARÁ, utilizando-os exclusivamente para os fins de interesse deste, estritamente no desempenho das atividades inerentes a prestação dos serviços contratados, não os revelando ou divulgando a terceiros, em hipótese alguma, sem o prévio e expresso consentimento do BANPARÁ;

V. Instalar e utilizar nos ambientes computacionais disponibilizados pelo BANPARÁ somente softwares desenvolvidos ou adquiridos pelo BANPARÁ;

VI. Permitir ao BANPARÁ a fiscalização, a qualquer tempo, de todos os dados manejados através dos meios fornecidos pelo BANPARÁ em razão da prestação de serviços contratados, pelo que autorizo o BANPARÁ a monitorar todos os dados manejados nos meios de propriedade do contratante, não configurando o referido monitoramento qualquer quebra de sigilo ou invasão de privacidade;

VII. Não utilizar o ambiente de internet disponibilizado pelo BANPARÁ para uso pessoal, ilícito, ilegal, imoral ou para quaisquer outros fins senão os de estrita prestação dos serviços contratados.

VIII. Declaro, ainda, para os devidos fins de direito, que me responsabilizo e obrigo a fazer com que quaisquer de meus agentes, empregados, consultores e demais colaboradores que vierem a ter acesso a quaisquer dados e informações confidenciais cumpram as obrigações constantes deste Termo.

Belém, de de 2015.

_____

Assinatura do contratado

ANEXO VII – MODELO DE DECLARAÇÃO DE INEXISTÊNCIA DE FATO IMPEDITIVA À HABILITAÇÃO

[Nome da empresa], CNPJ n.º _____sediada **[Endereço completo],** declara sob as penas da lei, que até a presente data, inexiste fato superveniente impeditivo para sua habilitação no presente processo licitatório, ciente da obrigatoriedade de declarar ocorrências posteriores.

_____

Local e Data

_____

Nome e Identidade do Declarante

ANEXO VIII – DECLARAÇÃO DE NÃO EMPREGAR MENOR

Declaramos, em atendimento ao previsto no Edital do Pregão Eletrônico nº , que não possuímos em nosso quadro de pessoal empregado com menos de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre e de 16 (dezesseis) anos em qualquer trabalho, salvo na condição de aprendiz, nos termos do inciso XXXIII do art. 7º da Constituição Federal de 1988.

Local e data.

Assinatura e carimbo do representante legal da empresa.

Local e data.

_____

Nome e Identidade do Declarante

ANEXO IX – ORÇAMENTO ESTIMADO

Contratação de empresa especializada, para Fornecimento de Solução Integrada de Serviços Gerenciados de Segurança compreendendo: provimento de serviços de proteção de perímetro interno e externo; monitoramento e administração dos serviços providos; gestão de conformidade e padrões; resposta a incidentes de segurança e transferência de conhecimento para o corpo técnico do BANPARÁ.

ITEM	DESCRIÇÃO	QTD	PREÇO UNITÁRIO	TOTAL (R$)
1	Serviço de Firewall Próxima Geração e VPN, fornecido com no mínimo 2 appliances em cluster ativo/ativo e um appliance de gerência (este de gerência podendo ser uma máquina virtual);	**48**	**R$ 29.387,91**	**R$ 1.410.619,68**
1.1	Inicialização dos Serviços da Solução de Firewall Próxima Geração e VPN	**1**	**R$ 477.694,70**	**R$ 477.694,70**
2	Serviço de Prevenção de Intrusos, fornecido com no mínimo 5 appliances, sendo 2 appliances em cluster ativo/failover para proteção da borda e 2 appliances em cluster ativo/failover para proteção da rede interna e 1 (um) appliance de gerência;	**48**	**R$ 48.422,81**	**R$ 2.324.294,88**
2.1	Inicialização do Serviço de Prevenção de Intrusos	**1**	**R$ 846.622,57**	**R$ 846.622,57**
3	Serviço de Gestão de Risco e Compliance fornecido com no mínimo 2 appliances, com capacidade e licenciamento para 2800 endereços IP;	**48**	**R$ 18.828,34**	**R$ 903.760,32**
3.1	Inicialização do Serviço de Gestão de Risco e Compliance	**1**	**R$ 338.332,11**	**R$ 338.332,11**
4	Serviço de Gateways de Email e Web fornecido com no mínimo 4 (quatro) appliances 2 (dois) em cluster ativo/ativo para o serviço de gateway de email e 2 (dois) appliances em cluster ativo/ativo para o serviço de gateway de web, licenciados para no mínimo 2000 usuários.	**48**	**R$ 20.257,28**	**972.349,44**
4.1	Inicialização do Serviço de Gateways Email e Web	**1**	**R$ 364.809,13**	**R$ 364.809,13**
5	Serviços de Proteção das Estações de Trabalho e Servidores de Rede fornecido com software licenciado para 2800 (dois mil e oitocentos) hosts;	**48**	**R$ 24.014,92**	**R$ 1.152.716,16**
5.1	Inicialização dos Serviços de Proteção das Estações de Trabalho e Servidores de Rede	**1**	**R$ 403.261,88**	**R$ 403.261,88**
6	Serviço de Proteção Contra Vazamento e Integridade dos Dados fornecido com no mínimo 3 appliances e software licenciado para 2800 (dois mil e quinhentos) hosts;	**48**	**R$ 59.390,06**	**R$ 2.850.722,88**
6.1	Inicialização dos Serviços de Proteção contra vazamento e integridade dos dados.	**1**	**R$ 1.116.204,46**	**R$ 1.116.204,46**

7	Serviço de Gestão de Eventos e Incidentes fornecido com no mínimo 1 (um) appliance;	**48**	**R$ 15.740,76**	**R$ 755.556,48**
7.1	Inicialização do Serviço de Gestão de Eventos e Incidentes	**1**	**R$ 283.457,15**	**R$ 283.457,15**
8	Serviço de Proteção Contra Ameaças Dia Zero fornecido com no mínimo 2 appliances em cluster ativo/ativo;	**48**	**R$ 29.561,65**	**R$ 1.418.959,20**
8.1	Inicialização do Serviço de Proteção Contra Ameaças Dia Zero	**1**	**R$ 565.233,42**	**R$ 565.233,42**
9	Serviço de Monitoramento e Proteção de Base de Dados	**48**	**R$ 30.941,60**	**R$ 1.485.196,80**
9.1	Inicialização do Serviço de Monitoramento e Proteção de Base de Dados	**1**	**R$ 525.846,38**	**R$ 525.846,38**
10	**TREINAMENTOS**			
10.1	Treinamento Firewall Próxima Geração e VPN	**1**	**R$ 47.628,97**	**R$ 47.628,97**
10.2	Treinamento de Prevenção de Intrusos	**1**	**R$ 47.628,97**	**R$ 47.628,97**
10.3	Treinamento Gestão de Risco e Compliance	**1**	**R$ 61.416,47**	**R$ 61.416,47**
10.4	Treinamento Gateway de Email e Web	**1**	**R$ 100.832,93**	**R$ 100.832,93**
10.5	Treinamento Proteção das Estações de Trabalho e Servidores	**1**	**R$ 100.832,93**	**R$ 100.832,93**
10.6	Treinamento Proteção contra Vazamento e Integridade dos Dados	**1**	**R$ 86.832,93**	**R$ 86.832,93**
10.7	Treinamento Gestão de Eventos e Incidentes	**1**	**R$ 39.541,47**	**R$ 39.541,47**
10.8	Treinamento Proteção Contra Ameaças Dia Zero	**1**	**R$ 50.416,47**	**R$ 50.416,47**
10.9	Treinamento Monitoramento e Proteção de Base de Dados	**1**	**R$ 54.416,47**	**R$ 54.416,47**
11	Banco de horas de serviços técnicos especializados	**4000 Hs**	**R$ 340,00**	**R$ 1.360.000,00**
TOTAL GLOBAL				**R$ 20.145.185,24**

Prazo de Vigência do Contrato de 48 (Quarenta e oito) meses, contados a partir de sua assinatura.

O licitante vencedor deve estar de pleno acordo com todas as condições e exigências estabelecidas no Edital e seus Anexos, bem como aceitamos todas as obrigações e responsabilidades especificadas no edital, termo de referência e contrato.

ANEXO X – MINUTA DE CONTRATO

INSTRUMENTO PARTICULAR DE CONTRATO DE **EMPRESA ESPECIALIZADA PARA FORNECIMENTO DE SOLUÇÃO INTEGRADA DE SERVIÇOS GERENCIADOS DE SEGURANÇA COMPREENDENDO: PROVIMENTO DE SERVIÇOS DE PROTEÇÃO DE PERÍMETRO INTERNO E EXTERNO; MONITORAMENTO E ADMINISTRAÇÃO DOS SERVIÇOS PROVIDOS; GESTÃO DE CONFORMIDADE E PADRÕES; RESPOSTA A INCIDENTES DE SEGURANÇA E TRANSFERÊNCIA DE CONHECIMENTO PARA O CORPO TÉCNICO DO BANPARÁ**, CONFORME AS DISPOSIÇÕES DESTE EDITAL E SEUS ANEXOS, QUE FAZEM ENTRE SI O BANCO DO ESTADO DO PARÁ S/A. E A XXXXXXXXXXXXXXXXXXXXXX, COMO ABAIXO MELHOR SE DECLARA:

Pelo presente instrumento particular que, entre si fazem, de um lado o **BANCO DO ESTADO DO PARÁ S.A.**, instituição financeira, com sede em Belém do Pará, na Avenida Presidente Vargas, n.º 251, Bairro Centro, CEP. 66.010-000, Belém–PA, inscrito no Ministério da Fazenda sob o CNPJ/MF n.º 04.913.711/0001-08, neste ato representado pelo seu Presidente **.....**, (qualificação), portador do Registro Geral n.º XXXXXXXXXXX e CPF/MF nº XXXXXXXXXXX e por seu(sua) Diretor(a) ....., (qualificação), portador(a) do Registro Geral nº. XXXXXXXXXXX e CPF/MF nº. XXXXXXXXXXX, ambos residentes e domiciliados nesta cidade, doravante designados CONTRATANTES e de outro lado, a XXXXXXXXXXX, com sede a XXXXXXXXXXX, inscritos no CNPJ/MF n. XXXXXXXXXXX, denominada **CONTRATADA**, neste ato representada por seu XXXXXXXXXXX, (qualificação), portador (a) do Registro Geral nº XXXXXXXXXXX e CPF/MF nº XXXXXXXXXXX, residente e domiciliado na XXXXXXXXXXX, celebram o presente Instrumento de Contrato, com Recursos Próprios do **CONTRATANTE**, consoante o **Processo Nº 1708/2015– SUSEM/GESEI**, por meio da licitação na modalidade Pregão Eletrônico, sendo todas as disposições contratuais regidas pelas Leis Federais Nº 8.666/1993, Lei nº. 10.520/2002, com suas alterações posteriores e, supletivamente, pelos Princípios da Teoria Geral dos Contratos e as disposições de Direito Privado, conforme cláusulas e condições a seguir:

CLÁUSULA PRIMEIRA – DO OBJETO

Constitui objeto deste contrato, a prestação de serviços de **CONTRATAÇÃO DE EMPRESA ESPECIALIZADA NO FORNECIMENTO DE SOLUÇÃO INTEGRADA DE SERVIÇOS GERENCIADOS DE SEGURANÇA LÓGICA, NO MODELO 24 HORAS POR DIA, 7 DIAS POR SEMANA, 365 DIAS POR ANO, INICIALMENTE POR 48 MESES, INCLUINDO O CONJUNTO DE HARDWARE E SOFTWARE FORNECIDOS EM REGIME DE COMODATO NECESSÁRIOS E SUFICIENTES PARA A PRESTAÇÃO DESSES SERVIÇOS**, CONFORME AS DISPOSIÇÕES DESTE EDITAL E SEUS ANEXOS.

PARÁGRAFO PRIMEIRO: Os serviços propostos deverão compor o seguinte escopo:

- Serviço de Firewall Próxima Geração e VPN, para controle do tráfego nos segmentos protegidos;
- Serviço de Prevenção de Intrusos, para detecção e bloqueio de intrusão nos segmentos protegidos;
- Serviço de Gestão de Risco e Compliance, para descoberta e gestão de eventuais falhas de segurança no ambiente;
- Serviço de Gateway de E-mail e Web, para controle do tráfego de e-mail e proteção contra vírus, spam e conteúdo indesejado, assim como para controle do tráfego de internet e proteção contra vírus, acessos indevidos e conteúdo indesejado;
- Serviço de Proteção das Estações de Trabalho e Servidores de Rede (Tanto físicos, quanto virtuais) para identificar e mitigar infecções por vírus;
- Serviço de Proteção Contra Vazamento e Integridade dos Dados, para identificar e mitigar possíveis perdas de informações sensíveis;
- Serviço de Gestão de Eventos e Incidentes, para armazenagem, gerenciamento e correlacionamento de logs e eventos;
- Serviço de Proteção Contra Ameaças Dia Zero, para identificar e bloquear esse tipo de ameaça no ambiente da CONTRATANTE;
- Serviço de Monitoramento e Proteção de Base de Dados, para monitorar, identificar e controlar acesso aos bancos de dados;

Disponibilização de banco de até 4.000 (mil) horas para a prestação de serviços técnicos, que possam ser utilizadas sob demanda.

PARÁGRAFO PRIMEIRO: Integra este pacto para todos os fins de direito, o Edital e seus anexos, Termo de Referência e anexos, bem como, a proposta de preços do CONTRATADO.

CLÁUSULA SEGUNDA: DAS OBRIGAÇÕES DA CONTRATADA

Além das obrigações contidas no Termo de Referência **– Anexo I do edital** e demais anexos, para o fiel cumprimento deste contrato, a **CONTRATADA** se obriga a:

a) Responsabilizarem-se pela adequada execução do contrato, com o atendimento integral das especificações, obrigações, exigências e condições inclusas no Termo de Referência e

anexos, à legislação e todas as normas vigentes relativas ao objeto contratado, bem como às necessidades e orientações do **CONTRATANTE**;

b) Dar ciência ao CONTRATANTE, imediatamente e por escrito, de qualquer anormalidade verificada na execução dos serviços;

c) Apresentar garantia nos moldes estabelecidos neste contrato;

d) Acatar todas as exigências do **CONTRATANTE**, sujeitando-se à ampla e irrestrita fiscalização, prestando todos os esclarecimentos solicitados e atendendo às reclamações formuladas;

e) Manter durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas no instrumento convocatório, bem como quanto ao cumprimento da Emenda Constitucional nº 42 à Constituição do Estado do Pará, de 04 de junho de 2008, devendo a empresa **CONTRATADA,** por ocasião da assinatura do Instrumento Contratual, apresentar Declaração de que emprega pessoas com deficiência, na forma prevista na referida Emenda;

f) Responsabilizar-se pelos empregados que colocar a disposição do CONTRATANTE, se for o caso, observadas as legislações trabalhistas e a Lei Previdenciária Social;

g) Responsabilizar-se pelos danos causados diretamente à administração ou a terceiros, decorrentes de sua culpa ou dolo, quando da execução dos serviços**,** não excluindo ou reduzindo essa responsabilidade a fiscalização ou o acompanhamento pelo **CONTRATANTE**;

h) Não ceder ou dar em garantia, a qualquer título, no todo ou em parte, os créditos de qualquer natureza decorrentes ou oriundos deste Contrato, salvo com autorização prévia e por escrito do **CONTRATANTE**;

i) Acatar as exigências do poder público, às suas expensas, as multas porventura impostas pelas autoridades competentes, mesmo aquelas que por força dos dispositivos legais sejam atribuídas ao **CONTRATANTE**, de tudo dando conhecimento a este;

j) Não subcontratar, no todo ou em parte, sem prévia anuência do **CONTRATANTE**.

k) Caso seja detectado qualquer problema na homologação do objeto do contrato, em qualquer uma das funcionalidades, a CONTRATADA deverá efetuar as devidas correções, sem qualquer ônus para a CONTRATANTE;

l) Não utilizar o nome do CONTRATANTE, ou sua qualidade de CONTRATADA em quaisquer atividades de divulgação empresarial, como, por exemplo, em cartões de visitas, anúncios diversos, impressos etc., sob pena de imediata rescisão do presente contrato, independentemente de aviso ou interpelação judicial ou extrajudicial, sem prejuízo da responsabilidade da CONTRATADA;

m)Garantir, por conta da execução deste contrato, através de ações de contingência, a continuidade dos serviços contratados, nos casos de impossibilidade de execução dos serviços pelos empregados da CONTRATADA;

n) Comunicar, verbal e imediatamente, ao **CONTRATANTE** todas as ocorrências anormais verificadas na execução dos serviços e, no menor espaço de tempo possível reduzir a escrito tal comunicação verbal apresentando-a ao citado órgão;

o) Realizar suas atividades utilizando profissionais regularmente contratados e habilitados, cabendo-lhe total e exclusiva responsabilidade pelo integral atendimento de toda legislação que rege os negócios jurídicos e que lhe atribua responsabilidades, com ênfase na previdenciária, trabalhista, tributária e cível.

p) Reembolsar o **CONTRATANTE** de todas as despesas que este tiver decorrentes de:

p.1) Reconhecimento judicial de titularidade de vínculo empregatício de prepostos seus com ao **CONTRATANTE**, ou qualquer empresa do mesmo grupo econômico;

p.2) Reconhecimento judicial de solidariedade ou subsidiariedade do **CONTRATANTE** ou qualquer outra empresa do mesmo grupo econômico no cumprimento das obrigações previdenciárias da **CONTRATADA**.

q) Responsabilizar-se, em caráter irretratável e irrevogável, por quaisquer reclamações trabalhistas ou qualquer outro ato de natureza administrativa ou judicial, inclusive decorrentes de acidente de trabalho, que venham ser intentadas contra o **CONTRATANTE**, por seus funcionários/colaboradores, que constituem mão-de-obra encarregada da execução dos serviços objeto deste contrato, seja a que titulo for e a que tempo decorrer, respondendo integralmente pelo pagamento de indenizações, multas, honorários advocatícios, custas processuais e demais encargos que houver, obrigando-se a **CONTRATADA** a requerer a substituição do **CONTRATANTE**.

PARÁGRAFO ÚNICO: A responsabilidade da **CONTRATADA** pela prestação de serviço, objeto desta licitação, não será reduzida ou alterada em decorrência da existência da fiscalização do **CONTRATANTE**. Deverá ser antes entendida como uma parceria responsável e de colaboração.

CLÁUSULA TERCEIRA – DAS OBRIGAÇÕES DO CONTRATANTE

Além das obrigações contidas no Termo de Referência e anexos– Anexo I do edital, para o fiel cumprimento deste contrato, o **CONTRATANTE** se obriga a:

a) Comunicar à **CONTRATADA** toda e qualquer ocorrência relacionada com a prestação dos serviços;

b) Acompanhar a prestação dos serviços objeto do presente contrato, por meio de servidor indicado, atestando ao final de cada etapa da prestação dos serviços e efetivar a satisfação do crédito da **CONTRATADA**, nos precisos termos dispostos no Contrato;

c) Prestar as informações e os esclarecimentos que venham a ser solicitados pela **CONTRATADA**;

d) Efetuar o pagamento na forma convencionada;

e) Proporcionar todas as facilidades para que a **CONTRATADA** possa desempenhar o fornecimento das licenças e o suporte dentro das normas propostas no edital de licitação e documentação pertinente a referida licitação;

f) Acompanhar e fiscalizar a prestação dos serviços por meio de servidor indicado e designado como seu representante.

PARÁGRAFO PRIMEIRO: A ausência ou omissão da fiscalização da **CONTRATANTE** não eximirá a **CONTRATADA** das responsabilidades oriundas deste contrato.

PARÁGRAFO SEGUNDO: A **CONTRATADA** autoriza o **CONTRATANTE** a descontar o valor correspondente aos danos ou prejuízos que causar, diretamente da fatura pertinente ao pagamento que lhe for devido.

CLÁUSULA QUARTA – DOS PREÇOS E CONDIÇÕES DE PAGAMENTO

O presente contrato tem o valor de R$ xxxxxxx, conforme abaixo especificado:

ITEM	DESCRIÇÃO	QTD	PREÇO UNITÁRIO	TOTAL (R$)
1	Serviço de Firewall Próxima Geração e VPN, fornecido com no mínimo 2 appliances em cluster ativo/ativo e um appliance de gerência (este de gerência podendo ser uma máquina virtual);	**48**		
1.1	Inicialização dos Serviços da Solução de Firewall Próxima Geração e VPN	**1**		
2	Serviço de Prevenção de Intrusos, fornecido com no mínimo 5 appliances, sendo 2 appliances em cluster ativo/failover para proteção da borda e 2 appliances em cluster ativo/failover para proteção da rede interna e 1 (um) appliance de gerência;	**48**		
2.1	Inicialização do Serviço de Prevenção de Intrusos	**1**		

3	Serviço de Gestão de Risco e Compliance fornecido com no mínimo 2 appliances, com capacidade e licenciamento para 2800 endereços IP;	**48**		
3.1	Inicialização do Serviço de Gestão de Risco e Compliance	**1**		
4	Serviço de Gateways de Email e Web fornecido com no mínimo 4 (quatro) appliances 2 (dois) em cluster ativo/ativo para o serviço de gateway de email e 2 (dois) appliances em cluster ativo/ativo para o serviço de gateway de web, licenciados para no mínimo 2000 usuários.	**48**		
4.1	Inicialização do Serviço de Gateways Email e Web	**1**		
5	Serviços de Proteção das Estações de Trabalho e Servidores de Rede fornecido com software licenciado para 2800 (dois mil e oitocentos) hosts;	**48**		
5.1	Inicialização dos Serviços de Proteção das Estações de Trabalho e Servidores de Rede	**1**		
6	Serviço de Proteção Contra Vazamento e Integridade dos Dados fornecido com no mínimo 3 appliances e software licenciado para 2800 (dois mil e quinhentos) hosts;	**48**		
6.1	Inicialização dos Serviços de Proteção contra vazamento e integridade dos dados.	**1**		
7	Serviço de Gestão de Eventos e Incidentes fornecido com no mínimo 1 (um) appliance;	**48**		
7.1	Inicialização do Serviço de Gestão de Eventos e Incidentes	**1**		
8	Serviço de Proteção Contra Ameaças Dia Zero fornecido com no mínimo 2 appliances em cluster ativo/ativo;	**48**		
8.1	Inicialização do Serviço de Proteção Contra Ameaças Dia Zero	**1**		
9	Serviço de Monitoramento e Proteção de Base de Dados	**48**		
9.1	Inicialização do Serviço de Monitoramento e Proteção de Base de Dados	**1**		
10	**TREINAMENTOS**			

10.1	Treinamento Firewall Próxima Geração e VPN	**1**		
10.3	Treinamento Gestão de Risco e Compliance	**1**		
10.4	Treinamento Gateway de Email e Web	**1**		
10.5	Treinamento Proteção das Estações de Trabalho e Servidores	**1**		
10.6	Treinamento Proteção contra Vazamento e Integridade dos Dados	**1**		
10.7	Treinamento Gestão de Eventos e Incidentes	**1**		
10.8	Treinamento Proteção Contra Ameaças Dia Zero	**1**		
10.9	Treinamento Monitoramento e Proteção de Base de Dados	**1**		
11	Monitoração e Administração de Segurança	**1**		
12	Serviços Técnicos Especializados	**1**		
TOTAL GLOBAL				

PARÁGRAFO PRIMEIRO: A inicialização da implantação de cada uma das soluções deverá ser comprovada pela CONTRATADA, através de testes efetuados pela sua Área de Segurança.

PARAGRAFO SEGUNDO: Os treinamentos especificados no item TREINAMENTOS, da planilha de preços (ANEXO II do edital), serão pago após a realização de todos os itens (01 a 12), em parcela única, paga em até 30 dias após a emissão do respectivo termo de aceite referente ao último treinamento efetuado.

PARÁGRAFO TERCEIRO: Parcela fixa mensal pela prestação dos serviços de manutenção e suporte técnico da solução, a ser paga até o décimo dia do mês subsequente da prestação do serviço, estando o pagamento da primeira parcela condicionada ao aceite da realização do treinamento, sendo que a cobrança deste serviço somente poderá ser iniciada após a implantação da solução.

PARÁGRAFO QUARTO: O pagamento à CONTRATADA será realizado, nos Termos do Termo de Referência e demais anexos, anexo a este Contrato.

PARÁGRAFO QUINTO: A CONTRATADA deverá apresentar nota fiscal/fatura devidamente atestada pela FISCALIZAÇÃO, observada as disposições constantes do Termo de Referência.

PARÁGRAFO SEXTO: As Notas Fiscais/Faturas e Documentação entregues em desacordo com esta cláusula serão devolvidas pelo **CONTRATANTE** com as informações que motivaram a rejeição, contando novo prazo para o efetivo pagamento.

PARÁGRAFO SÉTIMO: No preço apresentado pela licitante já estão incluídos todos os tributos e demais encargos que incidam ou venham a incidir sobre o contrato, assim como contribuições previdenciárias, fiscal e parafiscais, PIS/PASEP, FGTS, IRRF, emolumentos, seguro de acidente de trabalho, e outros, ficando excluída qualquer solidariedade do Banco, por eventuais autuações.

PARÁGRAFO OITAVO: Caso verificada a situação de descumprimento das condições de habilitação, nos termos do art. 55, inc XIII da Lei 8.666/93, será o CONTRATADO notificado para, em até 15 dias, regularizar a situação, sob pena de instauração de procedimento administrativo, com garantia de ampla defesa e contraditório, com finalidade de aplicação das penalidades previstas na Cláusula dez deste Contrato.

PARÁGRAFO NONO: Havendo necessidade de realização de serviços por profissionais residentes ou não residentes em Belém-PA, as despesas com passagens aéreas, deslocamentos, estadias e refeições, serão arcadas pela **CONTRATADA**.

PARÁGRAFO DEZ: A devolução da Nota/Fatura não servirá de pretexto ao descumprimento de quaisquer cláusulas contratuais.

PARÁGRAFO ONZE: O CONTRATANTE efetuará o pagamento via crédito em conta corrente a ser aberta pela CONTRATADA em uma das agências do Banco do Estado do Pará S/A - BANPARÁ, a qual deverá ser indicada na nota fiscal/fatura, conforme dispõe o Decreto do Estado do Pará nº 877/2008.

PARÁGRAFO DOZE: Todo e qualquer prejuízo ou responsabilidade, inclusive perante o Judiciário e órgãos administrativos, atribuídos ao CONTRATANTE oriunda de problemas na execução do contrato por parte da **CONTRATADA**, serão repassadas a esta e deduzidas do pagamento realizado pelo Banco, independente de comunicação ou interpelação judicial ou extrajudicial.

PARÁGRAFO TREZE: De acordo com a legislação tributária e fiscal em vigor, será efetuada a retenção na fonte dos tributos e contribuições incidentes no objeto contratado.

PARÁGRAFO CATORZE: A contratada se obrigará a utilizar a Nota Fiscal Eletrônica NF-e Modelo 55, em substituição a Nota Fiscal Modelo 1 ou 1-A (modelo antigo), na totalidade das operações de compras efetuadas pelas Unidades do CONTRATANTE, independente da atividade econômica exercida. Assim sendo, nenhuma nota fiscal modelo 1 ou 1-A será aceita, mesmo que dentro do prazo de validade de uso. Os demais modelos de notas fiscais e cupom fiscal continuam em vigor.

PARÁGRAFO QUINZE: Ocorrendo atraso no pagamento das faturas ou outros documentos de cobrança emitidos pela **CONTRATADA,** desde que não haja culpa da **CONTRATADA**, incidirá sobre os valores em atraso juros de mora no percentual de 1% (um por cento) ao mês, *pro rata die*, calculados de forma simples sobre o valor em atraso e devidos a partir do dia seguinte ao do vencimento até a data da efetiva liquidação do débito.

PARÁGRAFO DEZESSEIS: O CONTRATANTE poderá, a qualquer momento, solicitar à apresentação, pela CONTRATADA, no prazo de 10 (dez) dias, dos seguintes documentos, no original ou cópia autenticada:

a) Prova de quitação com as Fazendas Federal, Estadual e Municipal de seu domicílio ou sede;

b) Certidão negativa de débito do INSS – CND;

c) Certidão de regularidade de situação do FGTS – CRS;

d) Certidão negativa de falência, recuperação judicial ou extrajudicial;

e) Certidão quanto à dívida ativa da União;

f) Inscrição estadual e/ou municipal.

CLÁUSULA QUINTA – DA VIGÊNCIA CONTRATUAL E DE ACEITE DA NATUREZA DOS SERVIÇOS

O presente contrato terá vigência de 48 (quarenta e oito) meses, podendo ser prorrogado na forma da lei.

O objeto deste Contrato será recebido nos prazos e nos termos estabelecidos no Termo de Referência e demais anexos.

CLÁUSULA SEXTA - DA INEXISTÊNCIA DE VÍNCULO EMPREGATÍCIO

Fica, desde já, entendido que os consultores que prestam serviços para a **CONTRATADA** não possuem qualquer vínculo empregatício com o **CONTRATANTE**.

PARÁGRAFO PRIMEIRO: A **CONTRATADA** obriga-se a realizar suas atividades utilizando profissionais regularmente contratados e habilitados, cabendo-lhe total e exclusiva responsabilidade pelo integral atendimento de toda legislação que rege os negócios jurídicos e que lhe atribua responsabilidades, com ênfase na previdenciária, trabalhista, tributária e cível.

PARÁGRAFO SEGUNDO: A **CONTRATADA** obriga-se a reembolsar ao **CONTRATANTE** todas as despesas decorrentes de:

a) Reconhecimento judicial de titularidade de vínculo empregatício de prepostos seus com o **CONTRATANTE**, ou qualquer empresa do mesmo grupo econômico;

b) Reconhecimento judicial de solidariedade ou subsidiariedade do **CONTRATANTE** ou qualquer outra empresa do mesmo grupo econômico no cumprimento das obrigações previdenciárias da **CONTRATADA**.

PARÁGRAFO TERCEIRO: O **CONTRATANTE** não assumirá responsabilidade alguma pelo pagamento de impostos e encargos que competirem à **CONTRATADA**, nem se obrigará a restituir-lhe valores, principais ou acessórios, que esta, porventura, despender com pagamentos desta natureza.

CLÁUSULA SETIMA - FISCALIZAÇÃO E CONTROLE

Não obstante a **CONTRATADA** seja a única e exclusiva responsável pela execução do objeto ora contratado, o **CONTRATANTE** reserva-se o direito de, sem que de qualquer forma restrinja a plenitude desta responsabilidade, exercer a mais ampla e completa fiscalização da **CONTRATADA**, diretamente, pela SUSEM ou por outros prepostos especialmente designados.

PARÁGRAFO PRIMEIRO: O exercício de fiscalização pelo fiscal do **CONTRATANTE** não excluirá nem reduzirá as responsabilidades da **CONTRATADA**.

PARÁGRAFO ÚNICO: Ao **CONTRATANTE** fica desde já assegurado o direito de:

a) Solicitar à **CONTRATADA** o afastamento ou a substituição de qualquer de seus empregados, associados ou de propostos, por ineficiência, incompetência, má conduta ou falta de respeito a seus dirigentes, seus empregados ou terceiros;

b) Determinar o que for necessário à regularização das falhas ou defeitos observados;

c) Rejeitar todo e qualquer serviço de má qualidade ou não especificado, exigindo sua substituição ou correção imediatas;

d) Impugnar todo e qualquer serviço feito em desacordo com as especificações, normas regulamentares, legais e contratuais;

e) Ordenar a suspensão dos serviços, sem prejuízo das penalidades a que ficar sujeita a **CONTRATADA** e sem que esta tenha direito à indenização, caso, dentro de 48 (quarenta e oito) horas a contar da entrega da notificação correspondente, não seja atendida qualquer reclamação por falha ou incorreção no serviço prestado.

CLÁUSULA OITAVA – DO SIGILO DAS INFORMAÇÕES

A **CONTRATADA** assume total responsabilidade, inclusive por seus associados e colaboradores, em manter absoluto e irrestrito sigilo sobre o conteúdo das informações que digam respeito ao BANPARÁ, que vier a ter conhecimento por força da prestação dos serviços ora contratados, vindo a responder, portanto, por todo e qualquer dano que o descumprimento da obrigação aqui assumida venha a ocasionar ao BANPARÁ.

PARÁGRAFO PRIMEIRO: Todo e qualquer documento, informação ou material obtido e/ou fornecido a **CONTRATADA** pelo BANPARA será obrigatoriamente devolvido ao banco após a conclusão do serviço.

PARÁGRAFO SEGUNDO: A **CONTRATADA** guardará e fará com que seu pessoal guarde absoluto sigilo sobre dados, informações e documentos fornecidos pelo BANPARÁ, sendo vedada toda e qualquer reprodução dos mesmos.

PARÁGRAFO TERCEIRO: Todas as informações, resultados, relatórios e quaisquer outros documentos obtidos e/ ou elaborados pela **CONTRATADA** na execução dos serviços ora contratados, serão de exclusiva propriedade do BANPARÁ, não podendo a **CONTRATADA** utilizá-los para qualquer fim, ou divulgá-los, reproduzi-los ou veiculá-los, a não ser que prévia e expressamente autorizada pelo BANPARÁ.

CLÁUSULA NONA - DAS NOTIFICAÇÕES

Toda e qualquer notificação será feita por expediente registrado com comprovante de recebimento das áreas abaixo discriminadas, passando automaticamente a integrar este instrumento para todos os efeitos, valendo-se integralmente como documento aplicável, desde que os documentos sejam assinados pelos titulares das áreas abaixo indicadas, desde já reconhecidas como áreas interlocutoras oficiais para a operacionalização do objeto deste contrato.

PARÁGRAFO ÚNICO: A notificação enviada de acordo com o especificado acima será considerada como recebida na data indicada no comprovante de recebimento, ajustando-se como endereços para troca de correspondência e notificação os seguintes:

a) do CONTRATANTE:

SUSEM ...
END. .....
Att. .....
Telefone: (91) ....
Fax: (91) .....
E-MAIL: .....
b) da CONTRATADA:

CLÁUSULA DEZ - DAS PENALIDADES

No caso de atraso injustificado, execução parcial ou inexecução do contrato, a CONTRATADA ficará sujeita, sem prejuízo das responsabilidades civil e criminal, ressalvados os casos devidamente justificados e comprovados, a critério da administração e ainda garantida prévia e ampla defesa, às seguintes cominações administrativas, cumulativamente ou não, com as penalidades previstas neste instrumento, sem prejuízo da apuração das perdas e danos:

a) Advertência;

b) multa;

c) suspensão temporária de participar de licitações e impedimento de contratar com o BANPARÁ, por prazo não superior a 05 (cinco) anos;

d) declaração de inidoneidade para licitar ou contratar com a administração Pública, enquanto perdurarem os efeitos normativos da punição ou até que seja promovida a reabilitação.

PARÁGRAFO PRIMEIRO: A sanção de advertência poderá ser aplicada nas seguintes hipóteses:

a) descumprimento parcial das obrigações e responsabilidades assumidas contratualmente, inclusive no que se refere às disposições do art. 55, inc XIII da Lei 8.666/93, referente à obrigação de manter, durante todo o contrato, as mesmas condições de habilitação e qualificação exigidas na licitação;

b) outras ocorrências que possam acarretar transtornos ao desenvolvimento dos serviços do CONTRATANTE, a critério do CONTRATANTE, desde que não caiba aplicação de sanção mais grave.

PARÁGRAFO SEGUNDO: Em caso da não implementação dos serviços no prazo previsto, sem justificativas aceitas pelo BANPARÁ, serão aplicadas as seguintes penalidades:

a) Desconto de 0,25% (zero vírgula vinte e cinco por cento) do valor global do contrato, por dia de atraso na conclusão da implantação da solução, dedutível do valor da fatura de implantação (item 13.1.1 do termo de referência), limitados a 30 dias;

a.1) Após o 30º (trigésimo) dia de atraso, e a critério do BANPARÁ, poderá ocorrer a não aceitação do objeto, de forma a configurar, nessa hipótese, inexecução total da obrigação assumida, sem prejuízo da rescisão unilateral da avença.

b) Multa de 15% (cinco por cento) sobre o valor global da contratação no caso do adjudicatário/contratado deixar de realizar qualquer uma das obrigações abaixo relacionadas, configurando-se, tais casos, como inexecução total da obrigação assumida:

b.1) Assinar o contrato relativo ao objeto que lhe foi adjudicado, salvo se decorrente de motivo de força maior definido em Lei e reconhecido pela autoridade competente, ou entregar a declaração de que emprega pessoas com deficiência, na forma prevista na Emenda Constitucional nº 42, de 04 de junho de 2008, à Constituição do Estado do Pará

b.2) Cumprir fielmente as exigências estabelecidas no Termo de Referência e anexos, bem como as cláusulas contratuais,

b.3) Não abrir a conta corrente exigida na forma do Edital.

b.4) Responder pelos encargos fiscais e comerciais resultantes da adjudicação da licitação;

b.5) Responder, integralmente, por perdas e danos que vier a causar ao CONTRATANTE ou a terceiros em razão de ação ou omissão, dolosa ou culposa, sua ou dos seus prepostos, independentemente de outras cominações contratuais ou legais a que estiver sujeita;

b.6) Manter no curso do contrato, as condições de habilitação, o que será aferido periodicamente pelo CONTRATANTE, nos termos do art. 55, XIII da Lei nº 8.666/93.

PARÁGRAFO TERCEIRO: A multa por inexecução contratual poderá ser aplicada nos seguintes percentuais e situações:

a) de até 10% (dez por cento) pela inexecução/descumprimento parcial do contrato, calculada sobre o valor global do contrato, sem prejuízo de aplicação de outras penalidades;

b) de 15% (quinze por cento) pela inexecução/descumprimento total do contrato, calculada sobre o valor global do contrato, sem prejuízo de aplicação de outras penalidades;

c) Multa de 30% do valor global do contrato, no caso de rescisão por culpa da contratada, sem prejuízo de aplicação de outras penalidades;

d) Caso o percentual de atendimento seja inferior a 95% por três meses consecutivos do NMS especificado, será aplicada multa no valor de 1% (um por cento) do valor global do contrato.

PARÁGRAFO QUARTO: Caso prevista a situação de descumprimento do disposto no art. 55, inc XIII da Lei 8.666/93, poderá o Contratante aplicar multa por inexecução deste ajuste, em percentual de 10% (dez por cento) do valor mensal devido, até regularização da pendência.

PARÁGRAFO QUINTO: As multas poderão ser aplicadas cumulativamente com as sanções de advertência, suspensão temporária ou declaração de inidoneidade.

PARÁGRAFO SEXTO: A aplicação das multas acima não obsta que o CONTRATANTE rescinda unilateralmente o instrumento contratual e aplique as demais sanções.

PARÁGRAFO SÉTIMO: O valor da multa, a critério do CONTRATANTE, poderá ser descontado do(s) pagamento(s) a ser efetuado à CONTRATADA, independentemente de comunicação ou interpelação judicial, observando-se:

a) Se o valor a ser pago à CONTRATADA não for suficiente para cobrir o valor da multa fica a CONTRATADA obrigada a recolher a importância devida no prazo de 15 (quinze) dias, contado da comunicação oficial;

b) Em não sendo realizado o pagamento, a diferença devida poderá descontada da garantia contratual, e, na insuficiência desta, será objeto de cobrança judicial.

b.1.) Caso a garantia seja utilizada, no todo ou em parte para pagamento de multa, esta deve ser complementada no prazo de 10 (dez) dias.

c) Ao valor da multa não adimplida e objeto de cobrança judicial serão acrescidos honorários advocatícios, estes no percentual de 20%, custas judiciais, correção monetária (INPC) e juros na forma do art. 405 do Código Civil, facultando-se, ainda ao CONTRATANTE a inscrição do inadimplente nos órgãos de cadastro restritivo (SERASA/SPC).

PARÁGRAFO OITAVO: A suspensão do direito de licitar e contratar com o CONTRATANTE poderá ser aplicada à CONTRATADA se, por culpa ou dolo prejudicar ou tentar prejudicar a execução deste ajuste, nos seguintes prazos e situações:

a) por seis meses:

i) atraso no cumprimento das obrigações assumidas contratualmente, que tenha acarretado prejuízos financeiros para o CONTRATANTE;

ii) execução insatisfatória do objeto deste ajuste, se antes tiver havido aplicação da sanção de advertência, na forma do que dispõem o item 21.2 do edital.

b) por dois anos:

i) não conclusão dos serviços contratados ou não entrega dos bens contratados;

ii) prestação do serviço/fornecimento de bens em desacordo com o Termo de Referência e anexos, constante do Anexo I do edital, não efetuando sua correção após solicitação do CONTRATANTE;

iii) cometimento de quaisquer outras irregularidades que acarretem prejuízo ao CONTRATANTE, ensejando a rescisão do contrato por sua culpa;

iv) condenação definitiva por praticar, por meios dolosos, fraude fiscal no recolhimento de quaisquer tributos;

v) apresentação, ao CONTRATANTE, de qualquer documento falso ou falsificado, no todo ou em parte, com o objetivo de participar da licitação ou para comprovar, durante a execução do contrato, a manutenção das condições apresentadas na habilitação, bem como apresentar tipo de declaração falsa;

vi) demonstração, a qualquer tempo, de não possuir idoneidade para licitar e contratar com o CONTRATANTE, em virtude de atos ilícitos praticados;

vii) ocorrência de ato capitulado como crime pela Lei nº 8.666/93, praticado durante o procedimento licitatório, que venha ao conhecimento do CONTRATANTE após a assinatura do Contrato / Recebimento da Nota de Empenho;

viii) reprodução, divulgação ou utilização, em benefício próprio ou de terceiros, de quaisquer informações de que seus empregados tenham tido conhecimento em razão da execução desta contratação, sem consentimento prévio do CONTRATANTE;

c) por cinco anos, nos termos do art. 7º da Lei nº. 10.520/2002, no caso da empresa convocada dentro do prazo de validade da sua proposta, não celebrar o contrato, deixar de entregar ou apresentar documentação falsa exigida para o certame, ensejar o retardamento da execução de seu objeto, não mantiver a proposta, falhar ou fraudar na execução do contrato, comportar-se de modo inidôneo ou cometer fraude fiscal sem prejuízo das multas previstas em edital e no contrato e das demais cominações legais.

PARÁGRAFO NONO: A declaração de inidoneidade poderá ser proposta ao Secretário de Estado da Fazenda quando constatada a má-fé, ação maliciosa e premeditada em prejuízo do CONTRATANTE, evidência de atuação com interesses escusos ou reincidência de faltas que acarretem prejuízo ao CONTRATANTE ou aplicações sucessivas de outras penalidades.

PARÁGRAFO DEZ: Verificado o descumprimento dos termos do Edital, Contrato/Nota de Empenho ou seus anexo, será instaurado procedimento administrativo pela autoridade competente, no qual será assegurado a ampla defesa e o contraditório, com prazos de defesa e recurso de 05 (cinco) dias úteis, a contar do recebimento de notificação.

PARÁGRAFO ONZE: A critério da Administração poderá ser realizada a retenção do valor da(s) multa(s), o qual, após a conclusão do processo administrativo, garantida ampla defesa, será devolvido devidamente corrigidos pelo índice da poupança, caso o julgamento seja favorável à CONTRATADA.

PARÁGRAFO DOZE: As penalidades serão obrigatoriamente registradas, e no caso de suspensão de licitar, a ADJUDICATÁRIA/CONTRATADA será descredenciada por igual período, sem prejuízo das multas previstas no edital e das demais cominações legais;

PARÁGRAFO TREZE: Os prazos de adimplemento das obrigações contratadas admitem prorrogação nos casos e condições especificados no § 1º do art. 57 da Lei nº 8.666/93, devendo a solicitação dilatória, sempre por escrito, fundamentada e instruída com os documentos necessários à comprovação das alegações, ser recebida contemporaneamente ao fato que ensejá-la, sendo considerados injustificados os atrasos não precedidos da competente prorrogação.

CLÁUSULA ONZE – DA RESCISÃO

O presente contrato poderá ser rescindido, nas seguintes hipóteses:

a) de comum acordo entre as partes, independente de qualquer motivo, mediante simples aviso prévio de 90 (noventa) dias a contar do recebimento da notificação;

b) por inadimplemento da **CONTRATADA** de quaisquer obrigações assumidas neste contrato, inclusive aquelas previstas no art. 55, inc XIII, da Lei 8.666/93, sem prejuízo das responsabilidades civil e penal cabíveis, inclusive o disposto na **Cláusula Dez – Das penalidades**;

c) Liquidação amigável ou judicial ou falência da **CONTRATADA**;

d) Transferência total ou parcial de obrigações assumidas neste contrato, sem prévia anuência do **CONTRATANTE**, por escrito;

e) Quando a alteração do contrato social da **CONTRATADA** prejudicar a execução do contrato, a critério do **CONTRATANTE**;

f) Suspensão temporária ou declaração de inidoneidade da empresa em licitar ou contratar com a Administração Pública.;

g) A **CONTRATADA** tenha sua idoneidade técnica ou financeira abaladas ou o seu controle acionário modificado de forma a prejudicar a fiel execução de suas obrigações contratuais;

h) Nas hipóteses previstas nos artigos 77, 78 e 79 da Lei 8.666/93, conforme o caso;

i) Nos demais casos previstos na legislação aplicável.

CLAÚSULA DOZE – DO REAJUSTE

Os valores contratados serão reajustados anualmente, a contar da data de assinatura deste contrato, no prazo da lei, segundo a variação acumulada do INPC do Instituto Brasileiro de Geografia e Estatística – IBGE, ou outro, na falta deste, que estiver estabelecido na legislação à época de cada reajuste.

CLAÚSULA TREZE – DA GARANTIA

Em garantia ao fiel cumprimento de todas as cláusulas e condições do presente contrato, a **CONTRATADA** optará por uma das modalidades de garantia previstas nos incisos de I a III, do parágrafo primeiro, do art. 56, da Lei Nº. 8.666/1993:

a) Caução em dinheiro ou em títulos da dívida pública, devendo este ter sido emitido sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil e avaliados pelos seus valores econômicos, conforme definido pelo Ministério da Fazenda.

b) Fiança bancária.

c) Seguro-garantia.

PARÁGRAFO PRIMEIRO: O comprovante da efetivação da garantia escolhida pela **CONTRATADA**, deverá ser apresentado ao **CONTRATANTE**, até a assinatura do Contrato, para verificação análise e demais providências, sob a pena de perder a **CONTRATADA**, o direito de contratar com o **CONTRATANTE**.

PARÁGRAFO SEGUNDO: O valor da garantia, equivalente a 5% do valor global do contrato, será prestado conforme abaixo:

a) Em se tratando de caução: será creditado em conta de poupança vinculada ao presente contrato, aberta na agência Belém Centro/BANPARA, em favor do BANCO DO ESTADO DO PARÁ S/A. à ordem da área gestora de contratos e pagamentos, podendo ser aplicada a títulos rentáveis, a crédito do **CONTRATANTE**, sendo que os acréscimos ao principal serão incorporados à caução;

b) Em se tratando de fiança bancária, em qualquer Instituição Financeira Oficial a critério da **CONTRATADA**;

c) Em se tratando de seguro garantia: em qualquer seguradora, a critério da **CONTRATADA**.

PARÁGRAFO TERCEIRO: O valor da garantia de que trata esta cláusula ficará bloqueado durante o prazo de vigência do Contrato, somente podendo ser movimentado pelo **CONTRATANTE** para cobertura de danos decorrentes do presente ajuste, independentemente de

notificação ou interpelação judicial ou extrajudicial, especialmente pela inexecução de que trata a cláusula dez, sem prejuízo das demais sanções legais ou contratuais.

PARÁGRAFO QUARTO: Na hipótese do valor caucionado permanecer intacto até o final do contrato, o **CONTRATANTE** restituí-lo-á acrescido dos rendimentos que forem creditados através da conta de poupança, 30 (trinta) dias após o encerramento da vigência do contrato.

PARÁGRAFO QUINTO: Caso haja reajuste do valor do contrato ou retirada pela ocorrência de fatos que ensejem a utilização de parte ou totalidade do valor da garantia pelo **CONTRATANTE**, para cobertura dos danos causados ou multas, fica a **CONTRATADA** obrigada a complementar no prazo de até 10 (dez) dias úteis o valor da garantia de modo a corresponder sempre a 5% (cinco por cento) do valor do contrato.

CLAÚSULA QUATORZE – DAS DISPOSIÇÕES GERAIS

A declaração de invalidade, nulidade, ilegalidade ou inexequibilidade de qualquer cláusula, termo ou disposição deste Contrato, não afetará, ou atingirá a validade, legalidade, ou exeqüibilidade das demais disposições, termos e cláusulas contidas neste Contrato ou no Contrato como um todo.

CLÁUSULA QUINZE - FORO

O foro da Comarca da Belém-PA será o competente para julgar qualquer questão relacionada ao presente contrato.

E por estarem justos e contratados, assinam o presente Contrato em 02 (duas) vias de igual teor e forma, na presença das testemunhas abaixo.

Belém (PA), de de 2016.

BANCO DO ESTADO DO PARÁ S. A.

_____

CONTRATADA

TESTEMUNHAS:

_____ _____

NOME: **NOME:**

CPF: **CPF:**