EDITAL
PREGÃO ELETRÔNICO Nº 004/2011

O **BANCO DO ESTADO DO PARÁ S. A**., por intermédio da Pregoeira designada pela Portaria N.º 004/2010 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, Decreto Estadual N.º 878/2008 e subsidiariamente, da Lei n.º 8.666/1993 e alterações posteriores, **FARÁ REALIZAR LICITAÇÃO NA MODALIDADE PREGÃO, NA FORMA ELETRÔNICA, 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: 04/02/2011
HORÁRIO DE BRASÍLIA: 11h (horário de Brasília)
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 estabelecidos no preâmbulo deste Edital, desde que não haja comunicação da Pregoeira em contrário.

1. DO OBJETO

1.1. O presente Pregão tem por objeto a **CONTRATAÇÃO DE EMPRESA ESPECIALIZADA NA PRESTAÇÃO DE SERVIÇOS GERENCIADOS DE SEGURANÇA LÓGICA, NO MODELO 24HS POR DIA, 7 DIAS POR SEMANA, 365 DIAS POR ANO, INICIALMENTE POR 36 MESES, INCLUINDO O CONJUNTO DE HARDWARE E SOFTWARE FORNECIDOS EM REGIME DE COMODATO, NECESSÁRIOS E SUFICIENTES PARA A PRESTAÇÃO DESSES SERVIÇOS,** conforme especificações técnicas, condições e exigências estabelecidos no termo de referência, anexo I deste edital, **de acordo com o seguinte escopo**:

- Serviço de Firewall/VPN, para controle do tráfego nos segmentos protegidos;
- Serviço de IPS (Sistema de Prevenção de Intrusos), para detecção e bloqueio de intrusão nos segmentos protegidos;
- Serviço de Gestão de Vulnerabilidades, para descoberta e gestão de eventuais de falhas segurança no ambiente;
- Serviço de Filtro de E-mail, para controle do tráfego de e-mail e proteção contra vírus, spam e conteúdo indesejado;

- Serviço de Gestão de Antivírus Corporativo para os servidores e estações de trabalho do BANPARÁ para identificar e mitigar infecções por vírus;
- Disponibilização de banco de até 6.000 (seis mil) horas para a prestação de serviços técnicos, que possam ser utilizadas sob demanda.

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 O USO DA EXPRESSÃO "CONFORME O EDITAL" E SIMILARES, SOB PENA DE DESCLASSIFICAÇÃO.

2. CONSTITUEM ANEXOS DO EDITAL E DELE FAZEM PARTE INTEGRANTE

Anexo I: Termo de Referência
Anexo II: Política de Segurança do Banpará
Anexo III: Termo de Confidencialidade, Zelo e Responsabilidade sobre os bens de informação do Banco do Estado do Para S.A.
Anexo IV: Termo de Aceite de Atividade
Anexo V: Atestado de Experiência na Prestação de Serviços de Porte Compatível com o Objeto deste edital
Anexo VI: Modelo de Proposta de Preços
AnexoVII: Modelo Declaração de Inexistência de fato superveniente
Anexo VIII: Modelo de Declaração que não emprega menor
Anexo IX: Declaração de Visita Técnica
Anexo X: Declaração de que está de acordo com a realização dos serviços
Anexo XI: Minuta de Contrato

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, na forma eletrônica, no horário de 09h às 14h.

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.

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 a 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.** As informações e/ou esclarecimentos serão prestados pela Pregoeira através do site **www.banparanet.com.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.

5.2 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, lhe aplicada à sanção nos termos da legislação vigente, 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;

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.

6. DO CREDENCIAMENTO E DA REPRESENTAÇÃO

6.1. Os licitantes interessados 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 global do item, 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 04/02/2011**, 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 a 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 previstos 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 PELA PREGOEIRA.**

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 vencedor, deverão constar, pelo menos, as seguintes condições, conforme modelo constante do Anexo VI deste 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) Prazo de Vigência do Contrato de 36 (trinta e seis) meses, contados a partir de sua assinatura.

d) Prazo de Entrega: 45 (quarenta e cinco) dias consecutivos, contados a partir da data da assinatura do contrato, em conformidade com o item 11 do Termo de Referência;

e) local de implantação dos serviços: A instalação dos equipamentos e sistemas que permitirão a prestação dos serviços., deverá ser executado 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, em conformidade com o item 10 do Termo de Referência- Anexo I do Edital.

f) Preços unitários e globais 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, 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. (ver modelo do anexo VI).

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

h) Deverão ser apresentadas juntamente com a proposta de preços, os seguintes documentos:

- Declaração de atendimento da LICITANTE aos requisitos especificados no item 3.1 do termo de referência (Infraestrutura dos centros de operações de segurança (SOC) deste documento, disponibilizando o ambiente para auditoria por parte do BANPARÁ;
- Certificados para fins de comprovação do item 3.2.5 do termo de referência;
- Declaração dos fabricantes das soluções, para fins de comprovação do item 3.3.2 do termo de referência;
- Comprovação, independentemente da descrição da proposta, de todas as características técnicas exigidas na especificação das soluções técnicas, através

de documentos cujas origens sejam exclusivamente o fabricante dos equipamentos, como catálogos, manuais, ficha de especificação técnica os páginas obtidas no site oficial dos fabricantes, sob a forma de volumes impressos ou em meio eletrônico (CD, DVD, etc.);

7.7.1 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;

7.7.2 Serão aceitos documentos em português ou inglês para comprovações técnicas;

7.7.3 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;

7.7.4. A não comprovação de alguma característica exigida levará a desclassificação do licitante.

7.7.5 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.

7.8 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, e outros, ficando excluída qualquer solidariedade do Banpará, por eventuais autuações.

7.9. 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.

7.9.1. 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.

7.10. 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).

7.11. 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 o Pregoeiro do disposto no art. 97 da Lei nº 8.666/93.

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

7.13. A apresentação da proposta implicará a plena aceitação, por parte do licitante, das condições estabelecidas neste Edital e seus Anexos.

8. DA SESSÃO PÚBLICA

8.1. A partir das **11h (horário de Brasília) do dia 04/02/2011** 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 seus subitens deste edital, que deverão estar em perfeita consonância com o objeto deste edital no presente Edital e seus Anexos.

8.2. 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.

9. DA FORMULAÇÃO DE LANCES

9.1. Somente as Licitantes que apresentaram proposta de preços em consonância com o item 1.4 e seus subitens poderão apresentar lances, exclusivamente por meio do Sistema Eletrônico, sendo o Licitante imediatamente informado do seu recebimento e respectivo horário de registro e valor.

9.2. Assim como as propostas de preços, os lances serão ofertados pelo **VALOR GLOBAL DA PROPOSTA.**

- O Total Geral do contrato, para 36 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 36 meses, do valor total do banco de horas, o valor total cobrado pelos treinamentos de todos os serviços.

- 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.

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

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

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

9.6. 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.

9.7. 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.

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

9.9. 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.

9.10. 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.

9.11. 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.

9.12. 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;).

9.13. 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.

10. DO ENCERRAMENTO DA ETAPA DOS LANCES VIA MEIO ELETRÔNICO.

10.1. 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.

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

10.3. CASO O PREÇO COTADO SEJA SUPERIOR AO ESTIMADO PARA A CONTRATAÇÃO, PODERÁ OCORRER A NÃO ACEITAÇÃO.

10.4. 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).

10.5. 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:

10.5.1. Será assegurado, 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;

10.5.2. 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 10.5.1, 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 10.5.1, será realizado sorteio entre elas para que se identifique aquela que primeiro poderá apresentar melhor oferta.

10.5.3 A microempresa e a empresa de pequeno porte mais bem classificada será convocada para apresentar nova proposta no prazo máximo de 5 (cinco) minutos após o encerramento dos lances, sob pena de preclusão.

10.5.4 Na hipótese da não-contratação nos termos previstos no subitem 10.5.2, o objeto licitado será adjudicado em favor da proposta originalmente vencedora do certame;

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

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

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

10.8. Se a proposta de preços não for aceitável ou se o licitante não atender às exigências habilitatórias, a Pregoeira examinará a proposta de preços subseqüente 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.

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

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

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

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

10.11. 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.

10.12. A proposta de preços original devidamente atualizada com o último lance deverá ser enviada, **VIA SEDEX,** para o BANCO DO ESTADO DO PARÁ S/A, no endereço Av. Presidente Vargas, 251 – 6º 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).

11. DOS CRITÉRIOS DE JULGAMENTO DA PROPOSTA DE PREÇOS

11.1. 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.

11.2. 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.

11.3. O empate entre dois ou mais licitante 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.

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

11.5. Não será motivo de desclassificação 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.

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

12. DA HABILITAÇÃO

12.1. 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:

12.1.1. 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.

12.1.2. 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;

12.1.3. ATESTADO OU DECLARAÇÃO DE CAPACIDADE TÉCNICA: A LICITANTE deve possuir atestado(s) de capacidade técnica, focados em prestação de Serviços Gerenciados de Segurança, 24x7x365, onde são ou foram prestados todos os serviços que compõem o objeto deste Edital: Firewall/VPN, IPS, Filtro de E-mail, Gestão de Vulnerabilidades e EndPoint Security, conferido por empresas públicas ou privadas. O(s) atestado(s) devem comprovar que a(s) rede(s) gerenciada(s) somam, pelo menos, 2.000 (dois mil) hosts;

- O LICITANTE deve ser parceiro qualificado de todos os fabricantes das soluções que serão gerenciadas (Firewall/VPN, IPS, Filtro de E-mail, Gestão de Vulnerabilidades e Endpoint Security).

12.1.4 Declaração de Visita Técnica **(modelo do anexo IX)** ou uma declaração emitida pelo próprio licitante **(modelo do anexo X)** 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 deste Pregão.

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

Certificação	Quantidade de Profissionais
Certified Information Systems Security Professional (CISSP)	02
ITIL Foundation Certified	02

Certificação	Quantidade de Profissionais
PMP – Project Management Professional	02
Certificação na solução de Firewall/VPN ofertada	01
Certificação na solução de IPS ofertada	01
Certificação na solução de Gestão de Vulnerabilidades ofertada	01
Certificação na solução de Filtro de E-mail ofertada	01
Certificação na solução de Antivírus da McAfee	01

- Comprovação de que o profissional é funcionário em regime CLT, sócio ou prestador de serviço, fornecendo cópia da carteira de trabalho ou Contrato/Estatuto Social da Empresa ou Contrato de prestação de serviços.
- Caso ocorra o desligamento de qualquer um dos profissionais exigidos no item 3.2.5 ou 3.2.5.1 durante a vigência do contrato, a empresa deverá providenciar um substituto, com as mesmas certificações, no prazo máximo de 15 dias.

12.1.4. **Habilitação jurídica**:

a) Registro comercial, no caso de empresa individual;

b) Ato constitutivo, estatuto ou contrato social em vigor (com todas as alterações posteriores), ou a consolidação, se houver, devidamente registrado, em se tratando de sociedades comerciais. No caso de sociedades comerciais ou sociedades por ações, deverão ser acompanhados de documentos de eleição de seus administradores, no qual deverá estar contemplado, dentre os objetivos sociais, a execução de atividades da mesma natureza ou compatíveis com o objeto da licitação;

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.

12.1.5. 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;

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.

12.1.6. 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 3 (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, igual ou 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:

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

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

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

b) Comprovação de possuir patrimônio líquido ou capital social de no mínimo de 10% (dez por cento) do valor estimado da contratação, a qual está estimada em R$-3.052.266,33.

c) Certidão negativa de Pedido 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.**

12.2. Os documentos necessários à habilitação quando estiverem desatualizados no Sistema SICAF ou quando não estiverem nele contemplados, deverão ser encaminhados via fax conforme os prazos estabelecidos no item 12.3. Da mesma forma, os originais, ou cópia autenticada em Cartório competente, ou publicação em Órgão da imprensa oficial dos referidos documentos, deverão ser encaminhados via SEDEX, nos termos do item 12.4 abaixo.

12.3. O Licitante que for declarado vencedor do presente Pregão, deverá encaminhar via fac-símile, para o número (91) 3224-0370 ou (91) 3210-3303 ou ainda para o e-mail cpl@banparanet.com.br, os documentos necessários para habilitação, a proposta de preços atualizada com o último lance (ver modelo do anexo VI) e juntamente, com os anexos, quando for o caso, 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 mesma.

12.3.1. A documentação a que faz referência o item 12.3, quando encaminhada via e-mail, deverá estar digitalizada, devidamente assinada.

12.3.2. Quando a proposta de preços e as declarações constantes dos itens 12.1.1 e 12.1.2 forem assinadas por um preposto da empresa que não seja seu sócio administrador ou proprietário, o licitante também deverá enviar via fax ou e-mail 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.

12.3.3. O licitante que deixar de encaminhar a documentação acima especificada no prazo definido pela Pregoeira será DESCLASSIFICADO do certame.

12.4. O licitante que for declarado vencedor do presente Pregão Eletrônico e que encaminhar os documentos de habilitação via fac-símile, deverá enviá-los 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 6º andar – Comércio – Belém –Pará – CEP- 66.010.000, em dias úteis, no horário de 10h às 16h.

12.5. 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;**

12.5.1 Havendo alguma restrição na comprovação da regularidade fiscal, será assegurado o prazo de 2 (dois) 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;

12.5.2. 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.

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

12.7. 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.

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

13. DA VISITA TÉCNICA

13.1 Para que 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;

13.2 AS EMPRESAS QUE NÃO FOREM PARA A VISITA TÉCNICA DEVERÃO APRESENTAR UMA DECLARAÇÃO (VER MODELO DO ANEXO X) NA FORMA ESTABELECIDA NO ITEM 12.1.4 DESTE PREGÃO, DE QUE ESTÃO DE ACORDO COM A REALIZAÇÃO DOS SERVIÇOS, NÃO TENDO QUALQUER DÚVIDA QUE VENHA A PREJUDICAR OU MODIFICAR OS QUANTITATIVOS E ESPECIFICAÇÕES INDICADAS NO TERMO DE REFERÊNCIA.

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

13.4 Local da visita técnica: Rua Municipalidade Nº 1036 – Bairro: Umarizal, CEP: 66050350, e na Matriz localizado na Av. Pte. Vargas Nº 251, Bairro: Centro, CEP: 66010000

13.5 A VISITA TÉCNICA SERÁ REALIZADA NO DIA: 31/01/2011, no horário de 09h30 ÀS 11H30, OCORRENDO PRIMEIRAMENTE NA MATRIZ E SEGUINDO PARA O COMPLEXO MUNICIPALIDADE.

13.6 Todos os custos decorrentes desta visita ao local de realização dos serviços, estão a cargo da empresa licitante, sem que caibam quaisquer indenizações, ressarcimentos ou compensações ao 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, 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 contra-razões 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 da 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 09h às 14h.

15. DA ADJUDICAÇÃO E DA HOMOLOGAÇÃO

15.1. A adjudicação e homologação somente serão efetivadas:

a) Se não houver manifestação dos 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 de 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.

16. DO PRAZO PARA ASSINATURA DO CONTRATO

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

16.2. A convocação de que trata o subitem anterior deverá ser atendida no prazo máximo de 5 (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 da licitante vencedora de assinar o contrato dentro do prazo estabelecido pelo BANPARÁ, caracteriza o descumprimento total das obrigações assumidas, sujeitando-a às penalidades legalmente estabelecidas.

17. DO PRAZO PARA PRESTAÇÃO DOS SERVIÇOS

17.1. Os serviços serão prestados na forma e nos prazos previstos no termo de referência, anexo I do edital, bem como, na minuta do contrato.

17.2. 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.

18. DO PAGAMENTO

18.1 O pagamento será efetuado 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, além das estabelecidas no item 10 do termo de referência anexo I deste edital:

a) Apresentação de nota fiscal/fatura devidamente atestada pela FISCALIZAÇÃO, acompanhada da Certidão Negativa de Débito – CND, emitida pelo INSS, e do Certificado de Regularidade do FGTS – CRF;

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

c) Na forma prevista no item 13.1 do Termo de Referência, desde que não haja fato impeditivo para o qual, de alguma forma, tenha concorrido a ADJUDICATÁRIA/CONTRATADA.

d) **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 PUBLICAÇÃO NA IMPRENSA OFICIAL DO ESTADO DO PARÁ DA HOMOLOGAÇÃO DO RESULTADO FINAL DA LICITAÇÃO.**

18.2 Nenhum pagamento será efetuado à ADJUDICATÁRIA/CONTRATADA enquanto pendente de liquidação qualquer obrigação, em especial, quando os documentos comprobatórios de situação regular em relação ao INSS e ao FGTS, apresentados em atendimento às exigências de habilitação, estiverem com a validade expirada, de modo que o pagamento ficará retido até a apresentação de novos documentos dentro do prazo de validade. Esse fato não será gerador de direito a reajustamento de preços ou a atualização monetária.

19. DAS PENALIDADES

19.1. O BANPARÁ poderá, garantida a defesa prévia, aplicar sanções administrativas à ADJUDICATÁRIA/CONTRATADA, nos termos dos arts. 86 e 87 da Lei 8.666/93 e na minuta de contrato.

19.2. O licitante que cometer as infrações estabelecidas em lei ficará impedido de licitar e contratar com a Administração Pública, pelo prazo de até cinco anos, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, sem prejuízo das multas previstas neste edital e das demais cominações legais.

19.3. As penalidades serão obrigatoriamente registradas no SICAF, e no caso de suspensão de licitar, o licitante deverá ser descredenciado por igual período, sem prejuízo das multas previstas no Edital e das demais cominações legais.

19.4. Os prazos de adimplemento das obrigações contratadas admitem prorrogação nos casos e condições especificados no § 1º do art. 57 da Lei n.º 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.

19.5 Em caso da não implementação dos serviços no prazo previsto, sem justificativas aceitas pelo BANPARÁ, ocorrerá:

18.5.1 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;

18.5.2 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.

18.5.3 Multa de 10% do valor global do contrato, no caso de inexecução total da obrigação, sem prejuízo de aplicação de outras penalidades;

18.5.4 Multa de 30% do valor global do contrato, no caso de rescisão por culpa da contratada, sem prejuízo de aplicação de outras penalidades;

18.5.5 Caso o percentual de atendimento seja inferior a 95% por três meses consecutivos do SLA especificado, será aplicada multa no valor de 1% (um por cento) do valor global do contrato.

20. DAS CONDIÇÕES DE CONTRATAÇÃO

20.1. A empresa vencedora da licitação**,** por ocasião 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.

21. DA FRAUDE E DA CORRUPÇÃO

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

22. DO FORO

22.1. 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.

23. DAS DISPOSIÇÕES FINAIS

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

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

23.3 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.

23.4 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;

23.5 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.

23.6 Nenhuma indenização ou ressarcimento serão devidos aos licitantes pela elaboração de proposta ou apresentação de documentos relativos a esta licitação.

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

23.8 Sem prejuízo das disposições contidas no Capítulo III – Dos Contratos da Lei n.º 8.666/93, o presente Edital e a proposta da ADJUDICATÁRIA serão partes integrantes da Nota de Empenho ou Contrato, conforme o caso, a ser firmada com a ADJUDICATÁRIA.

23.9 O Instrumento de Contrato a ser firmado com a adjudicatária poderá ser alterado (a) nos casos previstos no art. 65 da Lei n.º 8.666/93, desde que haja interesse da Administração Pública.

23.10 A Pregoeira, ou autoridade superior, poderá promover diligências destinadas a elucidar ou complementar a instrução do processo, em qualquer fase da licitação, fixando prazos para atendimento.

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

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

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

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

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

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

23.17 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.

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

23.19 O edital e seus anexos, além de poderem ser lidos e retirados através da internet nos sites www.comprasnet.gov.br, www.banparanet.com.br e www.compraspara.pa.gov.br poderão também ser obtidos no BANPARÁ, SITUADA Av. Presidente Vargas, 251 – 6º andar, no horário de 10 às 14h, em dias úteis.

23.20 Para consulta e/ou quaisquer outros esclarecimentos necessários ao perfeito entendimento deste edital, poderão ser obtidos junto à Comissão Permanente de Licitações, pessoalmente, no endereço Av. Presidente Vargas, 251 – 6º andar – Sala de licitações – Belém-Pa, ou através do telefone/fax (91) 3210-3303, entre 10h e 14h ou pelo email cpl@banparanet.com.br.

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

Belém-Pará, 24 de Janeiro de 2011.

Vera Morgado
Pregoeira

ANEXO I- TERMO DE REFERÊNCIA

1. OBJETO.

- Contratação de empresa especializada na prestação de serviços gerenciados de segurança lógica, no modelo 24hs por dia, 7 dias por semana, 365 dias por ano, inicialmente por 36 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/VPN, para controle do tráfego nos segmentos protegidos;
- Serviço de IPS (Sistema de Prevenção de Intrusos), para detecção e bloqueio de intrusão nos segmentos protegidos;
- Serviço de Gestão de Vulnerabilidades, para descoberta e gestão de eventuais de falhas segurança no ambiente;
- Serviço de Filtro de E-mail, para controle do tráfego de e-mail e proteção contra vírus, spam e conteúdo indesejado;
- Serviço de Gestão de Antivírus Corporativo para os servidores e estações de trabalho do BANPARÁ para identificar e mitigar infecções por vírus;
- Disponibilização de banco de até 6.000 (seis 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 realizar a implantação das soluções, 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 Firewall/VPN;

2.1.1.2. Serviço de IPS (Sistema de Prevenção de Intrusos);

2.1.1.3. Serviço de Gestão de Vulnerabilidades;

2.1.1.4. Serviço de Filtro de E-mail;

2.1.1.5. Serviço de Gestão de Antivírus Corporativo para os servidores e estações de trabalho do BANPARÁ;

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

2.1.3. 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);

2.1.4. 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;

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

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, sócio ou prestador de serviço 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. A CONTRATADA deverá disponibilizar, nas instalações do Banpará, o acesso de leitura ao Serviço de Gestão de Logs e/ou Eventos (SIEM) e do IPS, que permita aos técnicos do Banpará terem acesso, no mínimo, aos alarmes de eventos e de correlação dos logs gerados pelos dispositivos de tecnologia da informação e segurança lógica;

2.2.6. Para todos os serviços, a contratada deverá criar contas de usuários somente leitura para que a equipe técnica do Banpará possa acompanhar e compreender as configurações adotadas.

2.2.7. 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;

2.2.8. 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;

2.2.9. 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;

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

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

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

2.2.11.2. 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;

2.2.11.3. 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;

2.2.12. Manutenção das Regras e Políticas e versões dos softwares

2.2.12.1. 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;

2.2.12.2. 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;

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

2.2.12.4. 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;

2.2.12.5. 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;

2.2.12.6. 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;

2.2.13. Controle dos Serviços Realizados pela CONTRATADA

2.2.13.1. Para o controle e administração dos serviços realizados pela CONTRATADA, o BANPARÁ poderá nomear até 02 (dois) representantes autorizados a interagir com aquela. Tais representantes serão responsáveis por:

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

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

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

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

2.2.13.3. 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;

2.2.13.4. 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;

2.2.13.5. A CONTRATADA deverá ministrar Treinamento não oficial na cidade da CONTRATANTE, mas utilizando o mesmo conteúdo praticado pelos cursos oficiais, visando treinar a equipe do BANPARÁ quanto às funcionalidades e os recursos de cada produto que fazem parte da solução.

2.2.13.6. O treinamento deverá ser ministrado para 9 pessoas, no ambiente do Banpará, com carga horária praticado pelo cursos oficiais. O material do curso deverá ser em língua portuguesa, podendo ser em inglês no caso de indisponibilidade.

2.2.13.7. Todos os treinamentos deverão ser realizados e terminados 30 dias antes da fase de implantação dos serviços especificados.

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

2.2.13.9. Caso o treinamento de qualquer um dos serviços não satisfaça em termos técnicos, o termo de aceite não será emitido e a contratada deverá ministratar novamente o curso, corrigindo os problemas apontados, sem ônus ao Banpará.

2.2.13.10. O custo referente ao treinamento deverá está incluso no valor global do contrato e discriminado nas propostas dos licitantes, conforme **Anexo VI - Planilha de Preços**.

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

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

2.2.14. Armazenamento dos logs de auditoria:

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

2.2.14.2. 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.

2.2.15. Ocorrência de Incidentes

2.2.16. 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;

2.2.17. Serão considerados 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;

2.2.18. A CONTRATADA deverá comunicar imediatamente o BANPARÁ, para que possam ser tomadas ações preventivas, os casos de tentativas de acessos indevidos, de instalação de códigos maliciosos, ou de qualquer outra ação que venham por em risco a segurança do ambiente do BANPARÁ, sem sucesso, mas que seja detectada insistência por parte da pessoa mal intencionada;

2.2.18.1. 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;

2.2.18.2. 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.

2.2.19. Solução de Hardware e Software da CONTRATADA

2.2.19.1. 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;

2.2.19.2. A manutenção das licenças do hardware e software necessários, junto aos fabricantes, será de responsabilidade da CONTRATADA, devendo esta apresentar cópia autenticada das mesmas anualmente ao BANPARÁ;

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

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

2.2.19.5. O hardware e o software devem ser fornecidos em regime de comodato, exceto para o serviço de antivírus, pois o BANPARÁ já dispõe de tais licenças, do fabricante McAfee;

2.2.20. Serviço de Gestão de Antivírus Corporativo

2.2.20.1. Escopo:

2.2.20.1.1. Gerência de 2.000 dispositivos (servidores de rede e estações de trabalho), utilizando as licenças de antivírus já adquiridas pelo BANPARÁ, contemplando:

2.2.20.1.2. Alteração e inclusão de regras

2.2.20.1.3. Alteração de configurações

2.2.20.1.4. Atualização do antivírus

2.2.20.1.5. Atualização (implementação de patches e fixes)

2.2.20.1.6. Atuação remota para resolução de problemas

2.2.20.1.7. Atuação local para resolução de problemas

2.2.20.1.8. Apresentação de relatório mensal técnico

2.2.20.1.9. Apresentação relatório emergencial

2.2.20.2. Serviço

2.2.20.2.1. Gerenciar a proteção na camada de Estações, Notebooks e Servidores.

2.2.20.2.2. Características gerais

2.2.20.2.2.1. Gerenciar a proteção aos seguintes sistemas operacionais: Windows 2000 Professional, Windows XP Professional, Windows 2000/2003 Server, Windows Vista 32 e 64 bits, Windows 7 32 e 64 bits, Windows Server 2008, Linux RedHat e Debian.

2.2.20.2.2.2. Acompanhar a detecção e remoção de todos os tipos de códigos maliciosos (malwares) incluindo Vírus, Spywares, Adwares; Graywares, Worms, Trojans, Rootkits, Hijackers e Keyloggers;

2.2.20.2.3. Características relacionadas à Administração

2.2.20.2.3.1. Acompanhar o status da última política de controle de epidemia (outbreak) e da política em andamento dos seguintes tipos:

2.2.20.2.3.1.1. Vírus / Malware;

2.2.20.2.3.1.2. Spyware / Grayware;

2.2.20.2.3.1.3. Firewall Violation;

2.2.20.2.4. Características relacionadas ao gerenciamento

2.2.21. Gerenciar o status atualizado das estações de trabalho, com as seguintes informações: data das vacinas, versão do antimalware, nome da máquina, status da conexão e IP;

2.2.21.1.1.1. Gerenciar a atualização automática dos arquivos de vacina contra malwares (update), dos mecanismos de verificação/correção (engine) e dos programas do sistema (upgrade);

2.2.21.1.2. Características relacionadas ao gerenciamento dos códigos maliciosos

2.2.21.1.2.1.1. Acompanhar a detecção e remoção de malwares de macro em tempo real;

2.2.21.1.2.1.2. Notificar o administrador em caso de epidemia de malwares;

2.2.21.1.2.1.3. Acompanhamento da reparação de danos causados por malwares do tipo “Trojan Horse” para reestabelecimento de operacionalidade;

2.2.21.1.2.1.4. Aplicar políticas de prevenção contra possíveis epidemias para uma máquina, para um grupo composto de várias máquinas ou para o domínio composto por vários grupos;

2.2.21.1.3. Gerar relatórios mensais com as seguintes informações:

2.2.21.2.Vírus identificados;

2.2.21.2.1. Vírus não limpos;

2.2.21.2.1.1. Total de arquivos verificados;

2.2.21.2.1.2. Quantidade de arquivos bloqueados;

2.2.21.2.1.3. Quantidade de conteúdo violado;

2.2.21.2.1.4. Gráfico de vírus identificado por mês;

2.2.21.2.1.5. Gráfico de arquivos bloqueados por mês;

2.2.21.2.1.6. Gráfico de violação de conteúdo por mês;

2.2.21.2.1.7. Tipo de ação tomada;

2.2.21.2.2. Acompanhamento do Gerenciamento Centralizado

2.2.21.2.2.1. Acompanhar através do console de gerenciamento centralizado, a execução de tarefas de limpeza automática de códigos maliciosos existentes em registros

do sistema operacional, de processos em tempo real e arquivos executáveis, eliminados de forma definitiva sem a intervenção humana;

2.2.21.2.2.2. Gerenciar o plano de distribuição das atualizações aos demais produtos.

2.2.22. Encerramento dos Serviços de Monitoração Remota da Segurança

2.2.22.1. 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 30 dias de antecedência;

2.2.22.2. 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.

2.2.22.3. 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.

2.3. Disponibilização de um banco de até 6.000 (seis mil) horas de serviços técnicos, que podem ser utilizadas sob demanda, para a prestação dos seguintes serviços:

2.3.1. Aplicação de correções de segurança nos ativos do BANPARÁ, exceto naqueles fornecidos em comodato, de acordo com o objeto desta licitação;

2.3.2. Consultoria em segurança da informação para:

2.3.2.1. Elaboração de pareceres

2.3.2.2. Análise forense

2.3.2.3. Análises de segurança em elementos que estejam fora do escopo desta licitação

2.3.2.4. Capacitação em segurança da informação;

2.3.3. Não haverá imposição do número mínimo de horas, a ser atendido pela CONTRATADA, para cada solicitação de uso do banco de horas;

2.3.4. A CONTRATADA deverá atender a cada solicitação de uso do banco de horas em, no máximo, 15 dias corridos;

2.3.5. As despesas com passagens e hospedagem, alimentação e deslocamento para o uso do banco de horas já devem estar incluídas no preço da hora.

2.3.6. As horas utilizadas do Banco de horas deverão ser previamente autorizadas pelo BANPARÁ.

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 magnética 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 hospedados em dois data centers diferentes, de forma que a falha completa de um dos data centers não afete o funcionamento dos sistemas. Cada um dos data centers 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 magnética ou via rede, e em seguida eliminadas da base de dados da CONTRATADA;

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

3.1.1.4.4. Estar hospedados em dois data centers diferentes, de forma que a falha completa de um dos data centers não afete o funcionamento dos sistemas. Cada um dos data centers deve atender as seguintes especificações:

3.1.1.4.4.1.1. 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.

3.1.1.4.4.2. Possuir caminhos de distribuição de energia elétrica, fluidos e gases para refrigeração 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:

3.1.1.4.4.2.1. Cabine para recebimento de energia externa

3.1.1.4.4.2.2. Cabeamento de transmissão de energia

3.1.1.4.4.2.3. Quadros de distribuição

3.1.1.4.4.2.4. Dutos de água gelada

3.1.1.4.4.2.5. Cabos para conexões de rede

3.1.1.4.4.3. 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;

3.1.1.4.4.4. Possuir múltiplas conexões independentes para acesso a Internet. Cada conexão para acesso a 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 distancia 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 casso 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.

3.1.1.5.1.5. Funcione em regime 24 x7.

3.1.1.5.1.6. Possua sistema de refrigeração de conforto central.

3.1.1.5.2. Registrar todas as entradas e saídas mantendo o registro armazenado para consulta por ao menos 90 dias.

3.1.1.5.3. Filmar permanentemente toda a área armazenada mantendo as imagens armazenadas por mais de 90 dias.

3.1.1.5.4. Possuir UPS que suporte todos os equipamentos essenciais ao funcionamento por, pelo menos, 30 minutos.

3.1.1.5.5. 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;

3.1.1.5.6. 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
Certified Information Systems Security Professional (CISSP)	02
ITIL Foundation Certified	02
PMP – Project Management Professional	02

Certificação	Quantidade de Profissionais
Certificação na solução(software) de Firewall/VPN ofertada	01
Certificação na solução(software) de IPS ofertada	01
Certificação na solução(software) de Gestão de Vulnerabilidades ofertada	01
Certificação na solução(software) de Filtro de E-mail ofertada	01
Certificação na solução(software) de Antivírus da McAfee	01

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

3.2.4.2. Caso ocorra o desligamento de qualquer um dos profissionais exigidos no item 3.2.5 ou 3.2.5.1 durante a vigência do contrato, a empresa deverá providenciar um substituto, com as mesmas certificações, no prazo máximo de 15 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 todos os serviços que compõem o objeto deste Edital: Firewall/VPN, IPS, Filtro de E-mail, Gestão de Vulnerabilidades e EndPoint Security, conferido por empresas públicas ou privadas. O(s) atestado(s) deve(m) comprovar que a(s) rede(s) gerenciada(s) somam, pelo menos, 2.000 (dois mil) hosts;

3.3.2. A LICITANTE deve ser parceiro qualificado de todos os fabricantes das soluções que serão gerenciadas (Firewall/VPN, IPS, Filtro de E-mail, Gestão de Vulnerabilidades e Endpoint Security).

3.4. Outras Características

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

4. SLA (ACORDO DE NÍVEL DE SERVIÇO)

4.1. Os tempos máximos de resolução especificados nas tabelas 2 a 6 devem ser seguidos, sob pena de multa:

4.1.1. Serviço de Firewall/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
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: SLA para serviço de Firewall/VPN

4.1.2. Serviço de IPS (Sistema 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

Atividade	Tempo de Máximo de Resolução
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 Períodico Técnico	Mensal
Relatório Emergencial	24 horas após o evento, desde que solicitado pelo BANPARÁ

Tabela 3: SLA para serviço de IPS

4.1.3. Serviço de Gestão de Vulnerabilidades

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

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 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: SLA para serviço de Gestão de Vulnerabilidades

4.1.4. Serviço de Filtro de E-mail

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

Atividade	Tempo de Resolução Máximo
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: SLA para serviço de Filtro de E-mail

4.1.5. Serviço de Gerenciamento de Antivírus Corporativo

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 do antivírus	Console: 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 para os casos citados nos itens 2.2.16.2 e 2.2.18.1.7	24 horas após abertuda de chamado ou detecção pelo SOC
Troca de equipamentos	24 horas após abertuda de chamado ou detecção pelo SOC
Relatório periódico técnico	Mensal
Relatório emergencial	24 horas após o evento, desde que solicitado pelo BANPARÁ

Tabela 6: SLA para serviço de Antivírus Coorporativo

4.2. Em casos emergenciais, quando houver a paralização nas atividades do negócio ou uma demanda de nível superior, o BANPARÁ poderá abrir chamados emergenciais, com o SLA 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 7: SLA para serviços emergenciais

4.3. Os SLAs, especificados nas tabelas 2 a 7, 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/VPN e de IPS, 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 vírgura 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 Filtro de E-mail 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 Antivírus Corporativo e de Gestão de Vulnerabilidades, 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 SLA (Acordo de Nível de Serviço) fazem parte do objeto deste Termo de Referência deverão ter meta de atendimento de, no mínimo, 98% (noventa e oito 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 SLA no mês;

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

5.6.3. Subtrai-se o número de chamados do serviço atendidos dentro do SLA no mês pelo número chamados do serviço atendidos fora do SLA 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 comprendido 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 comprendido 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 inicio 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 4 – Descrição dos Níveis de

Serviço 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. ESPECIFICAÇÃO DAS SOLUÇÕES TÉCNICAS.

6.1. Solução de Firewall/VPN

6.1.1. Hardware

6.1.1.1. 02 (dois) equipamentos de firewall novos de primeiro uso e 01 (um) equipamento dedicado para gerência. Esses Firewalls podem trabalhar no modo Ativo-Ativo.

6.1.1.2. Deve ser do tipo appliance com hardware e software do mesmo fabricante.

6.1.1.3. Deve possuir pelo menos 08 (oito) interfaces Gigabit Ethernet;

6.1.1.4. Deve permitir a criação de, no mínimo, 256 VLANs;

6.1.1.5. Deve possuir throughput de firewall de, no mínimo, 3 Gbps;

6.1.1.6. Deve possuir throughput de VPN de, no mínimo, 500 Mbps;

6.1.1.7. Deve suportar, no mínimo, 1.000.000 (um milhão) sessões concorrentes de firewall;

6.1.1.8. O sistema operacional do appliance deve suportar autenticação de usuário externas através de protocolos RADIUS ou TACACS, e não deve exigir contas de usuário local a ser criado no sistema operacional, com exceção de um administrador para usar em caso de uma falha no servidor RADIUS ou TACACS;

6.1.1.9. O sistema operacional deve implementar "forte" política de senha de usuário, com os seguintes requisitos:

6.1.1.9.1. Deve ser capaz de impor um tamanho mínimo e os diferentes tipos de caracteres (números, letras, caracteres especiais);

6.1.1.9.2. Deve ser capaz de forçar mudanças de senha periódica;

6.1.1.9.3. Deve acompanhar o histórico de senhas “velhas”, para evitar a reutilização das últimas 3 senhas (mínimo);

6.1.1.9.4. Deve implementar o bloqueio de conta de usuário depois de várias tentativas de login sem sucesso;

6.1.1.9.5. Deve implementar o bloqueio de conta de usuário / desabilitar para usuários sem tentativas de login após longos períodos de tempo (alguns dias).

6.1.1.10. A configuração do sistema operacional e monitoramento deve suportar a administração baseada em funções, uma vez que esta é uma maneira mais granular de conceder e administrar os privilégios do usuário e, ao mesmo tempo é uma maneira de ajudar nos processos de auditoria, todos baseados em perfis de acesso a recursos com base na função do usuário requisitos;

6.1.1.11. O sistema operacional deve suportar uma forma de configurar um aviso de login (por exemplo, um aviso aviso legal de que o acesso ao sistema é permitido apenas a pessoas autorizadas), a ser exibido na sessão de login (terminal), console local (terminal) ou todas as telas do terminal remoto do usuário antes de autenticação;

6.1.1.12. Alta Disponibilidade deve ser implementada no sistema operacional, permitindo que ambos ativo / standby e ativo / ativo na arquitetura de cluster, com todos os nós compartilhando os status das conexões e informação e em caso de falha de um nó de cluster, o impacto não é perceptível para os utilizadores e aplicações;

6.1.1.13. A plataforma de hardware deve suportar arquiteturas de clusters implementadas com balanceadores de carga externa ("Firewall balanceadores de carga");

6.1.1.14. Deve implementar o gerenciamento de segurança no nível do sistema operacional através de SSH / SCP, SSL e IKE / IPSec, para permitir o gerenciamento remoto total do appliance. Além disso, SSH e SSL, onde os protocolos utilizados na gestão do appliance deve permitir o máximo de proteção do protocolo sendo requerido o SSL versão 3 e versão 2 do protocolo SSH suportados pelos clientes;

6.1.1.15. Deve implementar pelo menos dois métodos de sincronização do relógio, incluindo suporte ao protocolo NTP para sincronização à base externas;

6.1.1.16. Deve suportar atualizações automático do horário de verão e também permitir iniciar e finalizar a customização através da interface do sistema operacional de configuração (GUI ou CLI);

6.1.1.17. Deve suportar VLAN 802.1Q tagging através de trunking com dispositivos de rede, para que cada VLAN ID configurada logicamente seja ligada à interface lógica diferentes no sistema operacional diferente. Cada interface executando a VLAN tagging também deve suportar o tráfego non-tagged, ao mesmo tempo;

6.1.1.18. Deve suportar agregação de link (802.3ad) em interfaces Ethernet. Essa implementação deve considerar uma forma de configurar o sistema operacional do appliance com um número mínimo de portas Ethernet física necessária sobre a “interface agregada” para manter

as exigências de serviço (para evitar problemas de largura de banda ou de transição HA desnecessária, no caso de uma configuração de cluster). Deve implementar o modo estático e o modo dinâmico (802.3ad Link Aggregation Control Protocol - LACP);

6.1.1.19. A plataforma de hardware e sistema operacional deve suportar uma tecnologia de redundância de interfaces Ethernet, onde os grupos são definidos na interface do equipamento e no caso de uma interface / link falhar, uma outra interface (stand by) se tornará ativo com o mesmo endereço IP e endereço MAC da anterior, desse modo os outros dispositivos de rede e as aplicações críticas não serão afetadas;

6.1.1.20. O sistema operacional deve implementar sistema de monitoramento e ferramenta de resolução de problemas, incluindo pacote de rastreamento capacidade para permitir a visibilidade de rede em tempo real no nível de sistema operacional e também ser capaz de filtrar essa captura de tráfego e armazená-los em formato libpcap binay e formato de texto;

6.1.1.21. Deve suportar mecanismo de agendamento de tarefas para as tarefas básicas de administração e frequentes, como a execução de scripts shell personalizado e copiar os arquivos;

6.1.1.22. Deve suportar o protocolo SNMP (versões 1, 2 e 3), incluindo traps de falhas de hardware e eventos (por exemplo, alterações na configuração do sistema operacional);

6.1.1.23. Deve suportar mecanismo interno para a compatilhamento/distribuição de tráfego entre os nós do cluster do appliance, de alta disponibilidade e escalabilidade de até 4 nós do cluster;

6.1.1.24. Deve permitir mais de uma versão instalada do sistema operacional e aplicativos de segurança (Firewall, VPN, etc) a qualquer momento, além das versões ativas;

6.1.1.25. A plataforma deve permitir que a MTU (unidade máxima de transmissão) seja customizadoa a fim de evitar a fragmentação de pacotes VPN;

6.1.1.26. A plataforma deve permitir que a MTU (unidade máxima de transmissão) seja customizada para permitir que valores superiores a 1500 bytes (também conhecido como Jumbo Frames), para melhorar o desempenho com interfaces Gigabit;

6.1.1.27. A plataforma deve permitir customização do MSS (Maximum Segment Size);

6.1.1.28. Deve suportar a aceleração de criptografia VPN através de processador dedicado;

6.1.1.29. Deve suportar protocolos de roteamento dinâmico (OSPFv2 e OSPFv2 NSSA, IGRP, RIPv2, BGP4), suportando a redistribuição de rotas, sumarização e filtragem. Deve suportar HA e configurações de cluster;

6.1.1.30. O sistema operacional deve suportar roteamento baseado em políticas, suportando a decisão de roteamento baseado em:

6.1.1.30.1. Endereço de origem

6.1.1.30.2. Comprimento da máscara de origem

6.1.1.30.3. Endereço de Destino

6.1.1.30.4. Comprimento da máscara de Destino

6.1.1.30.5. Porta de origem

6.1.1.30.6. Porta de destino

6.1.1.30.7. Tipo de Protocolo

6.1.1.31. Deve suportar protocolos de rotiamento multicast (DVMRP e PIM-DM).

6.1.1.32. A plataforma de hardware deve ser rack (rack 19 ") e suportar à gestão remota segura através da rede (ou seja, sem a necessidade de ter teclado, mouse e vídeo conectado ao aparelho);

6.1.2. Software

6.1.2.1. Características de Firewall

6.1.2.1.1. O gateway deve utilizar Stateful Inspection baseado em análise granular do estado da comunicação e da aplicação para acompanhar e controlar o fluxo da comunicação que passa por ele, abrindo portas para um grande conjunto de portas de maneira dinâmica e segura;

6.1.2.1.2. Deve suportar controle de acesso para pelo menos 150 aplicações/protocolos/serviços pré-definidos;

6.1.2.1.3. Deve proteger implementações de VoIP suportando H323 v2/3/4 (incluindo h.225 v2/3/4 e h.245 v3/5/7), SIP, MGCP e SCCP;

6.1.2.1.4. Deve incluir NAT dinâmico (N-1 ou Hide) e estático (1-1), com a possibilidade de converter os IPs de origem e destino e as portas no mesmo pacote com apenas uma regra;

6.1.2.1.5. Deve permitir a verificação de regras por intervalo de tempo;

6.1.2.1.6. A comunicação entre o servidores de gerenciamento e os gateways deve ser criptografada e autenticada;

6.1.2.1.7. O firewall deve suportar métodos de autenticação de usuário, cliente e sessão;

6.1.2.1.8. Deve autenticar sessões para qualquer protocolo ou aplicação baseada em TCP/UDP/ICMP;

6.1.2.1.9. Os seguintes esquemas de autenticação devem ser suportados pelos módulos de firewall e VPN: Tokens (como SecurID), TACACS, RADIUS, certificados digitais e dispositivos biométricos;

6.1.2.1.10. Deve incluir uma base de dados local que permita autenticação e autorização de usuários sem a necessidade de um dispositivo externo;

6.1.2.1.11. Deve suportar DHCP nos modos server e relay;

6.1.2.1.12. Deve ser capaz de trabalhar em Transparent mode (bridged mode);

6.1.2.1.13. Deve incluir a opção de controlar o acesso a compartilhamentos de arquivo Microsoft usando CIFS para permitir ao administrador decider quais pastas são acessíveis e quais não;

6.1.2.1.14. Deve suportar alta disponibilidade de gateways e balanceamento de carga com state synchronization;

6.1.2.1.15. A solução deve suportar pelo menos os seguintes protocolos de roteamento: BGP, OSPF, RIPv1 e RIPv2;

6.1.2.1.16. A solução deve suportar pelo menos os seguintos protocolos de multicast: IGMP, PIM-DM, PIM-SM;

6.1.2.1.17. Weighted Fair Queuing (WFQ) deve ser suportado a fim de alocar banda minima para um grupo de conexões ou para uma conexão específica;

6.1.2.1.18. A solução deve suportar prioridades por peso a fim de alocar banda de acordo com mérito;

6.1.2.1.19. A solução deve suportar limites de banda para definer restrições a aplicações de rede não-críticas;

6.1.2.1.20. Deve suportar Low latency queuing (LLQ) e Integrated Differentiated Services (DiffServ);

6.1.2.1.21. Deve suportar balanceamento de carga para servidor a fim de oferecer balanceamento de carga fácil na DMZ ou rede interna sem a necessidade de um balanceador externo. A solução também deve suportar pelo menos os seguintes métodos de balanceamento: Server Load, Round Trip, Round Robin, Random and Domain. Deve suportar pelo menos 150 serviços/aplicações pré-definidas;

6.1.2.1.22. Deve suportar alta disponibilidade e balanceamento de carga com pelo menos 2 ISP sem a necessidade de roteamento dinâmico ou equipamento externo específico;

6.1.2.2. Características de IPSec VPN

6.1.2.2.1. Deve suportar CA internas e CA externas de parceiros;

6.1.2.2.2. Deve suportar criptografia 3DES e AES-256 para IKE fases I e II;

6.1.2.2.3. Deve suportar pelo menos os seguintes grupos Diffie-Hellman: Grupo 1 (768 bit), Grupo 2 (1024 bit), Grupo 5 (1536 bit), Grupo 14 (2048 bit);

6.1.2.2.4. Deve suportar integridade de dados com md5 e sha1;

6.1.2.2.5. Deve incluir suporte para VPN site-to-site nas seguinte topologias: Full Meshed (todos para todos), Estrela (escritórios remotos para site central), Hub e Spoke (site remoto através de site central para outro site remoto).

6.1.2.2.6. Deve incluir suporte a client-to-site baseado em IPSEC;

6.1.2.2.7. Deve suportar SSL VPNs clientless para acesso remoto sem necessidade de instalação de um agente;

6.1.2.2.8. Deve suportar VPNs L2TP, incluindo suporte ao cliente L2TP nativo do iPhone;

6.1.2.2.9. O cliente IPSEC VPN incluso deve suportar roaming (mudança de redes/interfaces e mudança de endereço IP sem perda da conexão VPN) e Auto-Connect (uma conexão é feita automaticamente quando o endpoint está fora da rede corporativa e uma aplicação necessita acesso a essa rede);

6.1.2.2.10. Deve incluir uma maneira simples e central de gerencial VPNs, tornando possível criar várias VPNs ao mesmo tempo;

6.1.2.2.11. Deve permitir que o administrador aplique regras de segurança para controlar o tráfego dentro da VPN;

6.1.2.2.12. Deve suportar VPNs domain based e route based, usando pelo menos BGP e OSPF. (Requer a Blade de Advanced Networking);

6.1.2.2.13. Deve incluir um mecanismo para mitigar o impacto de um ataque DoS ao IKE, fazendo a distinção entre peers conhecidos e desconhecidos;

6.1.2.2.14. Deve incluir a funcionalidade para estabelecer VPNs com gateways com IPs públicos dinâmicos;

6.1.2.2.15. VPNs Deve incluir compressão de IP para VPNs client-to-site e site-to-site;

6.1.2.3. Gerenciamento de políticas de rede

6.1.2.3.1. A solução deve suportar perfis de administração distintos, incluindo pelo menos os seguintes perfis: read/write, read only, gerenciamento de usuários (com exceção de administradores) e visualização de logs;

6.1.2.3.2. Deve incluir um canal de comunicação segura com encriptação baseada em certificados entre todos os componentes da solução;

6.1.2.3.3. Deve incluir uma CA interna x.509 capaz de gerar certificados para gateways e usuários a fim de permitir fácil autenticação em VPNs;

6.1.2.3.4. Deve incluir a capacidade de confiar em CAs externas ilimitadas com a opção de verificar o certificado de cada gateway externo através de DN, IP, e-mail ou qualquer combinação;

6.1.2.3.5. A solução deve incluir um mechanismo de busca a fim de tornar fácil a consulta de quais objetos de rede contém IPs específicos ou parte deles. Deve também prover a opção de busca por objetos duplicados (Ex.: Com o mesmo IP) e objetos não utilizados (Ex.: Não usado em qualquer regra ou política) e listar em quais regras um determinado objeto é utilizado;

6.1.2.3.6. A solução deve incluir a opção de segmentar as regras de segurança através de rótulos a fim de melhor organizar as políticas;

6.1.2.3.7. Deve prover a opção de salvar versões de políticas manualmente e automaticamente;

6.1.2.3.8. Deve prover a opção de alta disponibilidade de gerenciamento, usando um servidor de gerência de standby que é automaticamente sincronizado com o ativo, sem a necessidade de um dispositivo externo;

6.1.2.3.9. A solução deve incluir um mapa detalhado com todos os objetos de rede e suas conexões que pode ser exportado para o Microsoft Visio ou uma imagem de arquivo;

6.1.2.3.10. A solução deve contar com a habilidade de distribuir e aplicar novas versões de software de gateway centralmente;

6.1.2.3.11. A solução deve incluir uma ferramente para gerencial centralmente as licenças de todos os gateways controlados pela estação de gerenciamento;

6.1.2.4. Logging & Status

6.1.2.4.1. O logging central deve ser parte do sistema (e não um syslog externo ou similares), e deve incluir a habilidade de facilmente

filtrar eventos baseado em diversas categorias (IP de fonte, porta de fonte, IP de destino, porta de destino, interface, categoria de ataque, translated IP, translated port e outros) ao mesmo tempo;

6.1.2.4.2. A solução deve prover logs diferentes para atividade comum de usuários e logs relacionados a gerência;

6.1.2.4.3. Para cada regra ou tipo de evento a solução deve fornecer pelo menos uma das seguintes opções de evento: Log, alerta, enviar um SNMP trap, enviar um email e executar um script definido pelo usuário;

6.1.2.4.4. Os logs devem ser transferidos de maneira segura entre o gateway e a gerência ou o servidor dedicado de log, e de lá até a console de visualização de logs no PC do administrador;

6.1.2.4.5. A solução deve incluir a opção de bloquear de maneira dinâmica uma conexão ativa desde a interface gráfica de visualização de logs sem a necessidade de modificar as regras;

6.1.2.4.6. A solução deve ser capaz de exporter logs para uma base de dados;

6.1.2.4.7. A solução deve suportar a troca automática de arquivo de log, de maneira regular ou através do tamanho do arquivo;

6.1.2.4.8. A solução deve ser capaz de associar um nome de usuário e o nome da máquina para cada usuário (IP interno) sempre que uma nova conexão for registrada. As informações devem ser obtidas a partir do Active Directory, sem a necessidade de adicionar um agente nem nos controladores de domínio, nem nos PCs dos usuários;

6.1.2.5. Monitoramento

6.1.2.5.1. A solução deve incluir uma interface de monitoramento gráfico que fornece uma maneira fácil de monitorar o status dos gateways;

6.1.2.5.2. A solução deve prover as seguintes informações do sistema para cada gateway: Sistema Operacional, consumo de CPU, consumo de memória, % de HD livre e atividade de rede;

6.1.2.5.3. A solução deve informar o status de todos os túneis de VPN, site-to-site e client-to-site;

6.1.2.5.4. A solução deve incluir um limite configurável que, quando atingido, deve iniciar uma determinada ação (ou ações). As ações devem incluir: Log, alerta, envio de um SNMP tral, envio de email e execução de um script definido pelo usuário;

6.1.2.5.5. Deve incluir gráficos pré-configurados para controle da evolução no tempo de informações do sistema, contadores de firewall, túneis VPN, tráfego de rede e outras informações úteis. Deve também fornecer a opção de gerar novos gráficos customizáveis de diferentes tipos;

6.1.2.5.6. Deve incluir a opção de reinicial um túnel VPN de maneira fácil e de desconectar um usuário remoto da interface gráfica;

6.1.2.5.7. A solução deve ser capaz de adicionar de maneira dinâmica regras de controle a fim de bloquear temporariamente pacotes baseado na fonte, destino e service desde a interface gráfica sem a necessidade de modificar as regras instaladas;

6.1.2.5.8. A solução deve ser capaz de monitorar perda de pacotes, uso de banda e atrasos entre dois pontos conectados via uma VPN, e logs e alertas quando um tunel de VPN estiver down;

6.1.2.6. Gerenciamento

6.1.2.6.1. A solução deve incluir uma maneira de acesso via browser para a visualização de políticas, objetos e usuários a fim de prover acesso para gerentes e auditores sem a necessidade de utilizar a console completa;

6.1.2.6.2. A solução deve oferecer a opção de autorizar e bloquear o acesso de usuários à visualização via browser;

6.1.2.6.3. A solução deve incluir suporte a SSL e porta configurável;

6.1.2.7. Diretório de Usuários

6.1.2.7.1. A solução deve ter integração com diretórios LDAP para autenticação e autorização de usuários baseado nos perfis armazenados no LDAP;

6.1.2.7.2. A solução deve incluir a opção de extender o schema de LDAP ou utilizar um modelo interno para as propriedades de usuários que não estão armazenadas no LDAP;

6.1.2.7.3. A solução deve incluir uma interface gráfica no gerenciamento do firewall para adição, remoção e edição de usuários armazenados no LDAP;

6.1.2.7.4. A solução deve incluir perfis pré-definidos e customizaveis para Microsoft AD;

6.1.2.7.5. Deve incluir a funcionalidade de pesquisar múltiplos servidores de LDAP para redundância e encontrar usuários distribuídos em múltiplos servidores de LDAP;

6.1.2.8. Workflow

6.1.2.8.1. Deve incluir um sistema de controle de mudanças incorporadas no servidor de gerenciamento;

6.1.2.8.2. Deve ser capaz de rastrear visualmente mudanças, destacando e enumerando todas as mudanças;

6.1.2.8.3. Deve ser capaz de gerar relatórios de todas as alterações feitas durante uma sessão, a ser utilizado pelos administradores e auditores;

6.1.2.8.4. Deve ser capaz de gerar relatórios comparativos entre duas sessões diferentes, resumindo todas as alterações feitas;

6.1.2.8.5. Deve ter a opção de forçar o administrador obter a aprovação de um gerente antes de instalar políticas;

6.2. Solução de IPS (Sistema de Prevenção de Intrusos)

6.2.1. Hardware

6.2.1.1. 02 (dois) equipamentos sensores e 01 (um) equipamento para gerência, novos e de primeiro uso;

6.2.1.2. Para o equipamento sensor:

6.2.1.2.1. Throughput (Taxa de Tranferência): no mínimo, 2 Gbps;

6.2.1.2.2. Quantidade de Interface de Monitoramento:

6.2.1.2.3. Cobre – no mínimo, 5 interfaces 1GB por Sensor

6.2.1.2.4. Possibilitar alternativa da configuração de interfaces non-failopen e failopen;

6.2.1.2.5. Latência na rede: menor que 2 milisegundos;

6.2.1.2.6. Suporte a bypass nas Interfaces de monitoramento;

6.2.1.2.7. Possuir capacidade de armazenamento;

6.2.1.2.8. Possuir fonte de Alimentação: Redundante;

6.2.2. Software

6.2.2.1. Filtrar de forma automática os falsos-positivos;

6.2.2.2. Funcionalidades de IPS/IDS;

6.2.2.3. Possibilitar visualização, edição e criação de regras;

6.2.2.4. Possibilitar personalizar workflow de visualização de dados;

6.2.2.5. Possuir base de dados incorporada;

6.2.2.6. Sistema de análise de vulnerabilidades embutidos de forma nativa no sistema. Este item poderá ser substituído se a solução de gestão de vulnerabilidades ofertada para atender o item 5.3 tiver integração com esta solução de IPS;

6.2.2.7. Suportar IPv6 nativo, e dentro do IPv6 tráfego tunneled dentro de pacotes IPv4;

6.2.2.8. Possuir Setup Wizard nativo;

6.2.2.9. Possibilitar ao cliente utilizar pacotes de latência thresholding, possibilitando automaticamente desativar temporariamente no caso de sensor in line;

6.2.2.10. Possuir multiplas políticas de IPS;
6.2.2.11. Oferecer proteção do dia-zero;
6.2.2.12. Possuir mais de 14.000 regras de IPS nativas únicas ou oferecer proteção contra o mesmo número de ataques;
6.2.2.13. As regras devem ser escritas no padrão Snort. Também serão aceitas plataformas que permitam a importação de regras no padrão Snort;
6.2.2.14. Possibilitar inspecionar a qualidade das assinaturas e regras. Soluções que permitam a customização de assinaturas de ataques e ofereçam o modo simulado de funcionamento do IPS, também serão aceitas;
6.2.2.15. Possuir Certificação NSS Labs;
6.2.2.16. A solução deve ser capaz de funcionar em modo passivo ou ativo simultaneamente em portas distintas;
6.2.2.17. A solução deve suportar opção de Fail-Open aceitando a passagem de tráfego mesmo com o sensor indisponível por qualquer motivo;
6.2.2.18. A solução deve ser baseada em sistemas operacionais “hardenizados”;
6.2.2.19. A solução deve usar autenticação forte e mecanismos de criptografia para todos os componentes da solução;
6.2.2.20. A solução deve ser inteiramente em appliances;
6.2.2.21. A solução tem que ser baseada em tecnologia padrão (não completamente ASIC), para que suporte novos protocolos sem a necessidade de alterar o hardware;
6.2.2.22. A solução deve monitorar a si própria e alertar quando anomalias físicas forem identificadas;
6.2.2.23. A solução deve monitorar a si própria em relação a ataques;
6.2.2.24. A solução deve enviar informação para SIEMs de forma criptografada sem utilizar softwares externos como VPNs, túneis de SSH, etc;
6.2.2.25. A solução deve guardar o estado de todas as sessões;
6.2.2.26. A solução deve remontar todos fluxos de pacote direcionados ao destino, para eliminar possíveis tentativas de evasão;
6.2.2.27. A solução deve possuir capacidade de inspeção profunda de pacotes (DPI), incluindo o payload, observando por tráfegos anômalos;
6.2.2.28. A solução deve permitir aplicação de novas políticas sem interrupção de trafego;

6.2.2.29. A solução deve permitir reinicialização do sensor sem interrupção de trafego;
6.2.2.30. A solução deve normalizar todas URLs para identificar ameaças a URLs especificas;
6.2.2.31. A solução deve prover estatística de pacotes descartados;
6.2.2.32. A solução deve prover a visualização da informação RAW, contendo o cabeçalho e o payload do pacote para fins de forensics, exportando a informação em formato pcap para análises posteriores;
6.2.2.33. A solução deve possuir configuração de “tresholds” para todos alertas identificados;
6.2.2.34. A solução deve prover a mesma linguagem para criação de regras que o Snort;
6.2.2.35. Deve prover updates regulares;
6.2.2.36. A solução não deve reescrever regras modificadas pelo usuário;
6.2.2.37. Deve possuir capacidade de identificar os pacotes referentes a uma dada regra;
6.2.2.38. A solução deve prover a criação dinâmica de regras;
6.2.2.39. Deve aceitar regras que aceitem a injeção de payloads alternativos em um dado pacote enviado a um determinado host;
6.2.2.40. Deve permitir a criação de assinaturas para protocolos não padrões;
6.2.2.41. Deve guardar informações sobre sessões, incluindo hora de inicio e final, portas, quantidade de informação, serviços (URL inclusa se HTTP).

6.3. Solução de Gestão de Vulnerabilidades

6.3.1. Hardware
6.3.1.1. 01 (um) equipamento novo e de primeiro uso.
6.3.1.2. O equipamento deve ter, integrado no mesmo, a engine de scan da rede, o banco de dados e o gerenciador;
6.3.1.3. Licença para varredura em até 2.500 (dois mil e quinhentos) endereços IPs;
6.3.1.4. Possuir arquitetura em modelo appliance;
6.3.1.5. Possuir, no mínimo, duas interfaces 10/100/1000Mbps Ethernet AutoSense;
6.3.2. Software
6.3.2.1. A ferramenta deve ter recurso para descoberta e criação de topologia dos ativos da rede. Entende-se por ativo da rede qualquer

computador, dispositivo, equipamento de rede que possua endereço IP, sem a necessidade de qualquer agente instalado nas estações;

6.3.2.2. A ferramenta deve ter a capacidade de se atualizar dinamicamente a partir do site do fabricante, possibilitando a descoberta das vulnerabilidades mais recentes;

6.3.2.3. A ferramenta deve apresentar os passos necessários para a realização da remediação das vulnerabilidades encontradas;

6.3.2.4. A ferramenta deve ter a capacidade de abrir e fechar chamados automaticamente em ferramentas de gerenciamento de tickets, para a realização de serviços de atualização manual;

6.3.2.5. A ferramenta deve possuir um mecanismo de pontuação que permita medir o nível de risco dos sistemas e dos recursos de rede da empresa;

6.3.2.6. Capacidade de trabalhar com diferentes níveis de usuários e com diferentes acessos;

6.3.2.7. A ferramenta deve ter a capacidade de definir o nível de criticidade de cada ativo para worms e exploits, auxiliando na do que é mais prioritário para ser remediado.

6.3.2.8. A ferramenta deve ter a capacidade de correlacionar os eventos baseados nos sistema operacional, porta, protocolo, banners e vulnerabilidades;

6.3.2.9. A ferramenta deve possuir uma arquitetura aberta e que permita interoperar com outros sistemas a partir de uma API específica, permitindo a integração mínima com os seguintes sistemas: Netegrity Siteminder, RSA Secure ID, LDAP;

6.3.2.10. Suportar os padrões CVE, IAVA & SANS/FBI Top 20;

6.3.2.11. A ferramenta deve ter a capacidade de detectar vulnerabilidades em dispositivos de redes sem fio, aplicações baseadas em Web, bases de dados, aplicações comerciais, sistemas operacionais e dispositivos de rede;

6.3.2.12. Toda a comunicação entre a console e o gerenciador deve ser encriptada, baseada em protocolo SSL;

6.3.2.13. Deve trabalhar com banco de dados integrado no appliance;

6.3.2.14. A ferramenta deve possuir a capacidade de criação de organizações e grupos com permissões de acesso distintas;

6.3.2.15. A ferramenta deve possibilitar a criação de diferentes tipos de relatórios baseados nos formatos: HTML padrão, CSV, XML e PDF;

6.3.2.16. Os relatórios e as varreduras devem ser configuradas para serem executados imediatamente, contínuo ou: diariamente, semanalmente ou mensalmente;

6.3.2.17. Os relatórios devem apresentar informações sobre o nível de risco de cada varredura, o risco por plataforma, o risco por vulnerabilidade;

6.3.2.18. Os relatórios devem ter no mínimo as seguintes informações: sumário, score com o nível de risco, topologia de rede descoberta, hosts descobertos, serviços descobertos, vulnerabilidades, detalhes sobre os dispositivos de redes sem fio descobertos, vulnerabilidades em windows, vulnerabilidades em aplicações web, informações de tendências e histórico de configuração;

6.3.2.19. Os alertas devem apresentar informações detalhadas sobre o nome da vulnerabilidade, descrição detalhada sobre a vulnerabilidade, os hosts afetados incluindo endereço IP, nome comum, os serviços abertos no host e as vulnerabilidades afetadas;

6.3.2.20. A ferramenta deve suportar o envio de alertas via email;

6.3.2.21. A ferramenta deve possuir a capacidade de verificações de vulnerabilidades: de uma forma não invasiva, invasiva, por tipo de risco, categoria, CVE e MS number;

6.3.2.22. O processo de verificação de vulnerabilidades em ambiente Windows deve incluir: detecção de hot fixes, service packs, registros, backdoors, trojans, peer to peer, antivírus, presença de modems nas estações;

6.3.2.23. O processo de verificação de vulnerabilidades em equipamentos wireless WiFi, deve ser capaz de descobrir equipamentos conectados via rede cabeada, descobrir o sistema operacional do dispositivo, detectar vulnerabilidades usando HTTP e SNMP;

6.3.2.24. O processo de verificação de vulnerabilidades em Web deve ser capaz de testar riscos de segurança em arquivos de dados, backups e diretórios por extensão .txt, .gz, .zip e .log, além de descobrir vulnerabilidades de SQL nas aplicações Web;

6.3.2.25. Os sistema deve ter a capacidade de configurar a velocidade da varredura de forma a não impactar a performance da rede;

6.3.2.26. As vulnerabilidades devem ser categorizadas em Alto, Médio, Baixo e Informativo;

6.3.2.27. Possuir uma linguagem de scripts que permita a criação de novas varreduras customizadas por usuário, de modo a somente mostrar os recursos disponibilizados para cada usuário.

6.4. Solução de Filtro de E-Mail

6.4.1. Hardware

02 (dois) equipamentos novos e de primeiro uso, para fins de redundância;

6.4.1.1. Licença para 2.000 (duas mil) caixas postais de correio eletrônico.

6.4.2. Software

6.4.2.1. Performance

6.4.2.1.1. Ser capaz de suportar, no mínimo, 10.000 conexões SMTP simultâneas;

6.4.2.2. Funcionalidades de Segurança

6.4.2.2.1. Sistema Operacional proprietário, customizado e desenvolvido para ser seguro e robusto de forma a suportar o produto de proteção para email;

6.4.2.2.2. Sistema de arquivos proprietário desenvolvido para otimizar as filas de mensagens;

6.4.2.2.3. MTA proprietário;

6.4.2.2.4. Criado com linguagem de programação que não utiliza pilhas (sem risco de vulnerabilidade a ataques do tipo estouro de pilha / “stack overflow”);

6.4.2.2.5. Possuir habilidade de controlar as sessões SMTP e limitar o tráfego de mensagens baseado em endereço IP, range de IPs, subnet IP, nome de domínio, nome parcial de domínio e reputação do emissor;

6.4.2.2.6. Ser capaz de restringir as conexões baseado em tamanho máximo de mensagem, número máximo de destinatários por mensagem, número máximo de mensagens por conexão e número máximo de conexões simultâneas por IP;

6.4.2.2.7. Ser capaz de restringir conexões baseado no número máximo de destinatários por hora;

6.4.2.2.8. Possibilitar limitar o número máximo de conexões simultâneas no Appliance;

6.4.2.2.9. Possibilitar o bloqueio ou engargalamento de maus remetentes e definir políticas individuais por remetente (tanto externo quanto interno) baseado em: IP Emissor, range de IP, domínio, reputação do emissor e lista DNS;

6.4.2.2.10. “Rate limit” controlado por endereço de IP, domínio ou reputação do Emissor;

6.4.2.2.11. Controle de máximo de destinatários trafegados por período de tempo;

6.4.2.2.12. Possibilitar definir o fluxo de tráfego baseado em períodos de tempo;

6.4.2.2.13. Checar DNS reverso e atribuir políticas;

6.4.2.3. Possibilitar configurar por política:

6.4.2.3.1. Habilitar TLS preferido ou obrigatório

6.4.2.3.2. Autenticação SMTP preferido ou obrigatório

6.4.2.4. Integrar com OpenLDAP, Active Directory ou outros servidores LDAP que possibilitem identificar usuários inválidos;

6.4.2.5. Rejeitar mensagens para destinatários inválidos durante o diálogo SMTP (prevenir Non-Delivery Report Attack);

6.4.2.6. Possibilitar o controle de bounce de e-mail;

6.4.2.7. Monitorar tráfego de mensagens em tempo real que permita identificar parâmetros críticos como volume de mensagens, histórico de conexões, conexões aceitas e rejeitadas, taxa de aceitação e de limites, filtros de reputação correspondentes, número de mensagens de spam positivos e suspeitos, número de vírus identificados;

6.4.2.8. Monitorar fluxo de mensagens em tempo real (detalhes do fluxo de mensagens por domínio e IP). Os fluxos de entrada e saída de mensagens devem ser exibidos separadamente;

6.4.2.9. Gerar estatísticas em tempo real de destinatários inválidos, bloqueados por reputação, Spams e Vírus encontrados, além das mensagens limpas (por domínio e IP);

6.4.2.10. Gerar estatísticas em tempo real de mensagens bloqueadas por “rate limit”, conexões rejeitadas, spams e vírus detectados na última hora, último dia, última semana e último mês, além dos bytes recebidos de acordo com o domínio ou IP;

6.4.2.11. O sistema de reputação deve utilizar dados de uma das maiores redes de monitoração de tráfego web e de email para definir a reputação dos remetentes, consultando um número mínimo de 100.000 redes participantes com cobertura global;

6.4.2.12. A rede de reputação não deve somente ser baseada em informações de fluxo da própria base de Appliances instalada, mas sim em inúmeros outros relatórios provenientes de: gaiolas de Spam, listas de URL, listas de equipamentos comprometidos, composição da mensagem, IPs em blacklist, volume global de trafego, listas brancas, composição da mensagem e web crawlers;

6.4.2.13. Possibilitar o controle de tráfego de Email por reputação atribuída pela rede de reputação, de cada IP que solicitou uma conexão. A rede de reputação deve monitorar no mínimo 90 parâmetros de Email e 40 de Web;

6.4.2.14. Suportar a verificação da autenticidade dos remetentes utilizando Domain Keys/DKIM/SPF/Sender ID;

6.4.2.15. Ser capaz de criar perfis de criptografia tanto para uso de servidores externos quanto servidores internos;

6.4.2.16. Ser capaz de criptografar mensagens localmente através de criação de regras que especifiquem quais mensagens devem ser criptografadas;

6.4.2.17. Ser capaz de criar perfis diferentes para cada uma das regras específicas de mensagens a serem criptografadas;

6.4.2.18. O método de criptografia utilizado não deve depender da instalação de softwares ou plugins na máquina do remetente e do destinatário;

6.4.2.19. O sistema deve gerar chaves por mensagem impossibilitando que a chave de uma mensagem possa abrir uma outra mensagem mesmo que para o mesmo destinatário;

6.4.2.20. Deve ser capaz de acessar servidor de chaves remoto através de Proxy;

6.4.2.21. Deve ter 2 (dois) níveis de segurança de acesso na leitura das mensagens criptografadas:

6.4.2.21.1. Nível alto: O receptor da mensagem deve entrar com credenciais de senha todas as vezes que abrir a mensagem mesmo que a senha esteja em cache;

6.4.2.21.2. Nível Médio: A senha não é requisitada se estiver em cache, ou seja caso o receptor tenha aberta a mensagem uma vez, não será necessário digitar novamente ao reabrir a mensagem enquanto a senha estiver em cache.

6.4.2.22. Deve usar no mínimo um dos seguintes algoritmos de criptografia: AES ou 3DES;

6.4.2.23. Deve permitir que os receptores das mensagens criptografadas possam responder e/ou encaminhar à mensagem de forma criptografada, para garantir a segurança da informação;

6.4.2.24. O sistema deve permitir que os templates das mensagens criptografadas possam ser customizadas;

6.4.2.25. As regras de mensagens a serem criptografadas podem ser criadas para estar de acordo com as normas de conformidade, tais como SOX;

6.4.2.26. O sistema deve proporcionar os seguintes controles das mensagens enviadas:

6.4.2.26.1. Permitir ao remetente configurar um tempo de expiração da chave (caso o tempo tenha expirado a mensagem não poderá ser aberta);

6.4.2.26.2. Permitir ao remetente cancelar a chave da mensagem antes mesmo que o destinatário a receba;

6.4.2.26.3. Enviar notificação de leitura da mensagem assim que o destinatário acesse a chave para abertura da mensagem;

6.4.2.27. As mensagens não deverão ser armazenadas no servidor de chaves ou no appliance de criptografia;

6.4.2.28. A mensagem deve ser entregue em um anexo criptografada e somente a chave deve ser transmitida entre o servidor e o destinatário em um acesso seguro do tipo SSL;

6.4.2.29. Possibilitar o envio de mensagens criptografadas sem a necessidade de uso de javascript;

6.4.3. Gerenciamento de Políticas

6.4.3.1. Suportar tráfego de entrada e saída no mesmo Appliance, mas possibilitar gerenciamento de políticas separadas;

6.4.3.2. Possibilitar atribuir diferentes endereços IP ao mesmo appliance, possibilitando a administração de diversos domínios com MXs diferentes, respeitando políticas diferenciadas para cada um deles;

6.4.3.3. Cada endereço IP deve oferecer respostas SMTP e banners diferenciados. (Ex.: 220 mx.exemplo.com.br para o IP A, 220 mx.outroexemplo.com.br para o IP B);

6.4.3.4. Possibilitar customizar o banner SMTP, o hostname e os códigos de resposta;

6.4.3.5. Suportar múltiplos domínios por endereço IP;

6.4.3.6. Permitir gerenciar políticas por usuário ou grupo de usuários (baseado em endereço/domínio de remetente/destinatário ou grupo do LDAP, exemplo: um único email enviado para diversos destinatários devem ser processados cada um por sua política específica);

6.4.3.7. Visão única de todas as políticas de usuários, para uma administração fácil e objetiva;

6.4.3.8. Controle de fluxo baseado em grupo de remetentes:

6.4.3.8.1. Blacklists (IP, Domínio, Reputação);

6.4.3.8.2. Whitelists (IP, Domínio, Reputação);

6.4.3.8.3. Possibilitar criação de vários grupos (por IP, domínio ou reputação);

6.4.3.8.4. RBLs/ORBLs proprietário ou de terceiros;

6.4.3.8.5. Whitelist e blacklist de endereços de remetentes e destinatários;

6.4.3.9. Identificação de arquivos anexos pelo tipo real do arquivo, pelo nome do arquivo, pela extensão e pelo MIME type;

6.4.3.10. Possibilidade de quarentenar, duplicar e quarentenar, remover o anexo, redirecionar as mensagens para outro host ou destinatário, substituir a mensagem inteira ou apenas o anexo com modelo de notificação pré-definido;

6.4.3.11. Verificação do remetente através do DNS reverso do IP de origem e através do endereço do remetente;

6.4.3.12. Suporte LDAP, para verificação de destinatários válidos;

6.4.3.13. A solução deve possuir um primeiro nível de filtro de conteúdo global que deve ser aplicado às mensagens antes das checagens de spam, de vírus e do segundo nível de análise de conteúdo;

6.4.3.14. As regras de filtragem devem suportar expressões regulares;

6.4.3.15. O segundo nível de filtro de conteúdo deve ser aplicável por usuário ou por domínio, analisando as mensagens de entrada e saída;

6.4.3.16. Os filtros devem ser aplicados baseados no remetente, destinatário, endereço IP, tamanho da mensagem, reputação, tipo de anexo, nome do anexo, tamanho do corpo da mensagem, listas públicas de blacklist, dicionários, assunto ou conteúdo no corpo da mensagem;

6.4.3.17. As regras de filtragem devem possibilitar múltiplas ações baseadas em múltiplas condições. As regras devem ser checadas em seqüência e possibilitar o uso de modelos para análise de entrada e saída;

6.4.3.18. Detectar objetos EXE, DLL, JPEG, GIF, BMP no mínimo dentro de arquivos como Excel e Word;

6.4.3.19. Possibilitar análise de conteúdo em arquivos do tipo PDF;

6.4.3.20. Permitir a configuração de relay confiável de forma que o IP de origem da mensagem possa ser identificado através do cabeçalho da mensagem (quando o appliance não é a primeira camada de checagem de mensagens);

6.4.3.21. Possibilitar converter mensagens HTML em texto;

6.4.3.22. Funcionalidades de bloqueio de Spam

6.4.3.22.1. Deve possuir filtro de Reputação (IP/Domínio do remetente);

6.4.3.22.2. Deve possuir filtros Reativos de AntiSpam;

6.4.3.22.3. Tecnologia de detecção deve ser sensível ao contexto;

6.4.3.22.4. Tecnologia deve englobar reputação de Email e Web;

6.4.3.22.5. Deve possuir técnica de aprendizado adaptativo;

6.4.3.22.6. Filtro AntiSpam deve ser integrado no Appliance;

6.4.3.22.7. Permitir que um usuário ou grupo de usuários utilize diferentes filtros AntiSpam;

6.4.3.22.8. Informações da rede de reputação também devem ser utilizadas para análise das mensagens, pelo filtro de AntiSpam, utilizado no appliance.;

6.4.3.22.9. Devem ser automáticas e atualizadas a cada 15 minutos;

6.4.3.22.10. Deve permitir mudar a política de mensagens em tempo-real para possíveis spammers e hackers (por domínio e endereço IP) para bloquear/engargalar esses possíveis maus remetentes;

6.4.3.22.11. Deve possuir quarentena no Appliance para administração;

6.4.3.22.12. Deve permitir acesso individual, com autenticação de usuário e senha, para cada quarentena;

6.4.3.22.13. Quarentena para usuário final deve suportar autenticação por LDAP/AD/IMAP/POP;

6.4.3.22.14. Deve enviar mensagens de notificação para o usuário final quando há mensagens de spam ou suspeitas na quarentena. Deve permitir ao usuário visualizar as mensagens na quarentena e entregar ou apagar as mensagens. A notificação dever ser personalizável e permitir o agendamento do envio para mais de uma vez ao dia, no mínimo;

6.4.3.22.15. Deve possibilitar armazenar as mensagens em quarentena no próprio Appliance ou em outro hardware especializado;

6.4.3.22.16. Deve possibilitar o uso de outro appliance de gerenciamento da quarentena do usuário final;

6.4.3.22.17. Deve possibilitar ao usuário final a criação de blacklists e safelists com os endereços que eles não querem e querem receber, respectivamente;

6.4.4. Funcionalidades do Antivírus

6.4.4.1. Deve ser integrada ao Appliance, permitindo que o administrador defina políticas diferenciadas por grupos de usuários;

6.4.4.2. Deve gerar relatórios e estatísticas específicos para esta funcionalidade;

6.4.4.3. Deve fornecer camada adicional de proteção dia-0 para surtos de novos vírus. No caso de surtos a solução deve armazenar em quarentena as mensagens que caracterizem risco por um período de tempo configurável ou até que as vacinas para os novos vírus sejam liberadas e aplicadas no antivírus, reduzindo o tempo de vulnerabilidade a surtos de novos vírus;

6.4.4.4. Deve permitir a configuração de exceções de acordo com a extensão do arquivo;

6.4.4.5. Os filtros de proteção devem permitir a configuração de acordo com os níveis de ameaças;

6.4.4.6. Todo o processo de proteção dia zero deve ser automático por regras enviadas ao appliance sem a necessidade da intervenção manual do usuário ou administrador;

6.4.4.7. Intervalo entre atualizações configurável em intervalos de tempo;

6.4.4.8. Checagem de arquivos:

6.4.4.8.1. Checagem de anexos;

6.4.4.8.2. Checagem de arquivos compactados;

6.4.5. Funcionalidades de Administração

6.4.5.1. Deve possuir monitoramento gráfico do fluxo de mensagens de entrada e saída da última hora, último dia, última semana e último mês;

6.4.5.2. Deve permitir log do processamento de cada mensagem;

6.4.5.3. Deve possuir relatório de fluxo de mensagens (Exemplo: possibilitar listar as mensagens para um destinatário específico em determinado período de tempo, com detalhes de como esta mensagem foi recebida, processada e entregue/apagada);

6.4.5.4. Deve gerar estatísticas de mensagens e performance;

6.4.5.5. O sistema deve fornecer logs de Antivírus, Antispam, mensagens, debug, sistema, escaneamento, linha de comando, erros, interface de gerência e status;

6.4.5.6. Possibilitar exportar dados para CSV e gerar arquivo PDF para armazenamento ou impressão;

6.4.5.7. Deve possuir relatórios com gráficos em formato de pizza e barras, que apóiem na comprovação do ROI;

6.4.5.8. Permitir o agendamento para envio automático de cada tipo de relatório (por dia, semana, mês), podendo distinguir para quem e qual relatório será enviado;

6.4.5.9. Permitir geração de relatórios por quantidade de dias ou meses desejados;
6.4.5.10. Deve possuir controle de acesso por quarentena;
6.4.5.11. Deve suportar diversas quarentenas configuradas separadamente;
6.4.5.12. Possibilitar que o acesso seja liberado apenas a usuários autorizados (Exemplo: quarentena “Confidencial” só pode ser acessada pelo Administrador);
6.4.5.13. Deve suportar tanto os servidores DNS raiz ou servidores locais;
6.4.5.14. Possibilitar desabilitar a verificação de DNS reverso para conexões de entrada;
6.4.5.15. Deve suportar configurações DNS que permita utilizar dois servidores de cache diferentes;
6.4.5.16. Deve suportar localização de mensagens, permitindo localizar por endereço de remetente/destinatário, domínio, assunto, período de tempo ou evento das mensagens no próprio appliance ou externamente para múltiplos Appliances;
6.4.5.17. Permitir gerar relatórios de todas as mensagens ou por grupos de domínios;
6.4.5.18. Permitir gerar relatório de volume de uso por usuário (maiores remetentes ou destinatários de vírus, spam, volume e tamanho de mensagens);
6.4.5.19. Permitir gerar relatórios de volume de uso por domínio (maiores domínios de entrada e saída de mensagens por volume, spam e vírus);
6.4.5.20. Permitir gerar relatório de violação de políticas ou filtro de conteúdo;
6.4.5.21. Permitir gerar relatório de eficiência da proteção dia-0;
6.4.5.22. Permitir gerar relatório dos maiores remetentes ou destinatários de vírus;
6.4.5.23. Permitir gerar relatório dos maiores remetentes ou destinatários de spam;
6.4.5.24. Permitir autenticação externa do tipo LDAP/RADIUS, para gerencia da solução.
6.4.5.25. Suportar monitoramento do sistema via SNMP v1/v2/v3, MIB-II, XML, Syslog;
6.4.5.26. Suportar API para desenvolvimento de relatórios personalizados.
6.4.5.27. Possuir alertas baseados em Emails, podendo especificar o tipo de alerta, a críticidade e para qual Email será enviado;
6.4.5.28. Enviar traps SNMP;
6.4.5.29. Possuir interface Web (HTTP e HTTPS);

6.4.5.30. Deve ser possível administrar via Linha de comando (SSH e Telnet);
6.4.5.31. Suportar gerenciamento centralizado para configurar e gerenciar múltiplos Appliances, sem necessidade de console dedicada para gerenciamento;
6.4.5.32. Permitir criar políticas por usuário, por grupo ou por Appliance;
6.4.5.33. Permitir habilitar um túnel seguro de suporte para diagnóstico e interações remotas;
6.4.5.34. Possibilitar testar a configuração efetuada antes que a mesma entre em produção para toda a rede;
6.4.6. Atualizações
6.4.6.1. Atualizações automáticas de Antispam;
6.4.7. Controle de Entrega
6.4.7.1. Monitoramento em tempo real do fluxo de entrega por domínio/IP;
6.4.7.2. Separar filas de entrega por domínio de destino;
6.4.7.3. Possibilitar adicionar diferentes rodapés ou disclaimers baseados em domínio, endereço de email e grupo de origem;
6.4.7.4. Suportar o envio de mensagens através de TLS por domínio de destino;
6.4.7.5. Suportar recebimento de mensagens através de TLS;
6.4.7.6. A solução deve gerar alertas de falhas de negociação TLS;
6.4.7.7. Deve gerar relatórios das conexões usando TLS;
6.4.7.8. Suportar autenticação SMTP para envio de mensagens;

7. VISITA TÉCNICA

7.1. 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;

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

7.3. A comprovação deverá ser através de uma Declaração de Visita Técnica (modelo do anexo IX) ou uma declaração emitida pelo próprio licitante (modelo do anexo X) 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. COMPROVAÇÕES – APRESENTAR COM A PROPOSTA DE PREÇOS

8.1 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.

8.2 Para fins de habilitação serão exigidas as seguintes comprovações técnicas:

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

8.2.2 Certificados para fins de comprovação do item 3.2.5 deste termo de referência;

8.2.3 Declarações conferidas por empresas públicas ou privadas, para fins de comprovação do item 3.3.1 deste termo de referência;

8.2.4 Declaração dos fabricantes das soluções, para fins de comprovação do item 3.3.2 deste termo de referência;

8.2.5 Atestado de Visita Técnica, para fins de comprovação do item 7 (VISITA TÉCNICA) deste termo de referência.

9 REQUISITOS OBRIGATÓRIOS GERAIS

9.2 A documentação exigida neste item deverá ser como anexo à **PROPOSTA DE PREÇOS**;

9.3 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 os páginas obtidas no site oficial dos fabricantes, sob a forma de volumes impressos ou em meio eletrônico (CD, DVD, etc.);

9.4 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;

9.5 Serão aceitos documentos em português ou inglês para comprovações técnicas;

9.6 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;

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

10 LOCAL DE IMPLANTAÇÃO DOS SERVIÇOS

10.2 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;

11 CONDIÇÕES DE ENTREGA E IMPLANTAÇÃO DOS SERVIÇOS

11.2 O prazo para entrega dos equipamentos e sistemas que compõem o serviço pela CONTRATADA será de 45 (quarenta e cinco) dias consecutivos, contados a partir da data da assinatura do contrato;

11.3 Os equipamentos e sistemas que compõem o serviço deverão ser entregues e instalados no BANPARÁ. As fases da implantação do serviço devem contemplar:

11.3.1 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.

11.3.1.1 Os prazos para a implantação de cada um dos serviços, pela CONTRATADA, estão especificados na tabela 8. 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/VPN	30
IPS	30
Gestão de Vulnerabilidades	30
Filtro de E-mail	30
Antivírus Corporativo	15

Tabela 8: Prazo para implantação dos serviços por categoria.

11.3.2 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.

11.3.3 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 exeqüível e ágil, caso ocorra alguma falha no processo de implantação dos controles necessários à prestação do serviço.

11.3.4 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 SLA acordado.

11.3.4.1 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);

11.3.4.2 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;

11.3.5 Documentação: A CONTRATADA deverá elaborar e manter atualizada documentação das atividades e de todos os processos.

11.3.5.1 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.

11.3.5.2 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.

12 VALOR DO SERVIÇO

12.2 A tarifação do serviço compreenderá os seguintes valores, a serem expressos em R$ (reais):

12.2.1 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;

12.2.2 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 36 meses;

12.2.3 Disponibilização de um banco de horas, a ser utilizado sob demanda;

12.2.4 Valor total para Treinamento de todos serviços especificado neste Termo.

12.3 O Total Geral do contrato, para 36 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 36 meses, do valor total do banco de horas, o valor total cobrado pelos treinamentos de todos os serviços.

12.3.1 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.

13 DO PAGAMENTO

13.2 Os pagamentos a serem realizados serão efetuados da seguinte forma:

13.2.1 Parcela única pela implantação da solução, sendo que esta parcela poderá ser paga em até 10 dias após a emissão de termo de aceite pelo BANPARÁ.

13.2.2 O pagamento referente à instalação, será realizado mediante a conclusão da instalação de todos os itens (01 a 05), constante na planilha de preço ANEXO VI do edital.

13.2.3 Parcela única pelo treinamento da solução, sendo que esta parcela poderá ser paga em até 10 dias após a emissão de termo de aceite pelo BANPARÁ.

13.2.4 Os treinamentos especificados no item TREINAMENTOS NÃO OFICIAIS, da planilha de preços (ANEXO VI do edital), serão pago após a realização de todos os itens (01 a 05).

13.2.5 Parcela fixa mensal pela prestação dos serviços de manutenção e suporte técnico da solução, a ser pago até o décimo dia do mês subseqüente 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.

13.2.6 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 10 dias do vencimento, ficando este isento de responsabilidade por atrasos na apresentação das faturas por parte da CONTRATADA.

13.2.7 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.

13.2.8 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.

13.2.9 A devolução da Nota/Fatura não servirá de pretexto ao descumprimento de quaisquer das obrigações da CONTRATADA.

13.2.10 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.

13.2.11 Nenhum pagamento será efetuado à CONTRATADA, enquanto pendente de liquidação qualquer obrigação financeira que lhe for imposta em virtude de penalidade ou inadimplência contratual.

13.2.12 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.

13.2.13 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.

13.2.14 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.

13.2.15 De acordo com a legislação tributária e fiscal em vigor, será efetuada a retenção na fonte dos tributos e contribuições incidentes no objeto contratado.

14 PENALIDADES

14.2 Em caso da não implementação dos serviços no prazo previsto, sem justificativas aceitas pelo BANPARÁ:

14.2.1 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;

14.2.2 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.

14.2.3 Multa de 10% do valor global do contrato, no caso de inexecução parcial da obrigação, sem prejuízo de aplicação de outras penalidades;

14.2.4 Multa de 15% do valor global do contrato, no caso de inexecução total da obrigação, sem prejuízo de aplicação de outras penalidades;

14.2.5 Multa de 30% do valor global do contrato, no caso de rescisão por culpa da contratada, sem prejuízo de aplicação de outras penalidades;

14.2.6 Caso o percentual de atendimento seja inferior a 95% por três meses consecutivos do SLA especificado, será aplicada multa no valor de 1% (um por cento) do valor global do contrato.

15 OBRIGAÇÕES E RESPONSABILIDADES DA CONTRATADA

15.2 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;

15.3 Manter Centros de Operação de Segurança (SOC) próprios para monitoramento remoto 24x7x365, com infraestrutura estritamente de acordo com as especificações deste documento;

15.4 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;

15.5 A CONTRATADA será responsável pela manutenção preventiva e corretiva dos hardwares e softwares por ela ofertados;

15.6 Todas as soluções de hardware e Software, ambientes de gerenciamento e monitoramento devem ser fornecidos em regime de comodato;

15.7 Iniciar a prestação dos serviços dentro dos prazos estabelecidos neste Termo de Referência;

15.8 Implementar/gerenciar backup de configuração de sistemas gerenciados;

15.9 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;

15.10 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;

15.11 As implantações das soluções serão realizadas pela CONTRATADA e todas as atividades envolvidas serão acompanhadas e coordenadas por analistas e técnicos do BANPARÁ;

15.12 Resolver os chamados de serviço e suporte técnico conforme os tempos definidos nas tabelas de tempos de atendimento (SLA) deste Termo de Referência;

15.13 Substituir equipamentos com defeito, que cause a indisponibilidade de serviço dependente do mesmo, conforme o tempo estipulado na tabela de tempos de atendimento (SLA);

15.14 Manter os serviços contratados nos níveis de disponibilidade estabelecidos em item específico deste Termo de Referência;

15.15 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);

15.16 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;

15.17 Quando previamente acordado entre as partes, a CONTRTADA poderá realizar serviços de monitoramento in loco com o acompanhamento de um representande do BANPARÁ.

15.18 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;

15.19 Produzir e enviar por e-mail, mensalmente, relatórios analíticos a equipe gestora do BANPARÁ, ou em 24h quando for demandado;

15.20 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;

15.21 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.

16 OBRIGAÇÕES E RESPONSABILIDADES DA CONTRATANTE

16.2 Providenciar as condições técnicas e ambientais necessárias à implantação e funcionamento dos serviços;

16.3 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;

16.4 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;

16.5 Cumprir pontualmente todos os seus compromissos financeiros para com a CONTRATADA;

16.6 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;

16.7 Comunicar à CONTRATADA todas as possíveis irregularidades detectadas na execução dos serviços contratados, para a pronta correção das irregularidades apontadas;

16.8 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;

16.8.1 Rejeitar, no todo ou em parte, a solução entregue pela CONTRATADA fora das especificações deste Termo de Referência;

16.8.2 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.

ANEXO II

POLÍTICA DE SEGURANÇA DO BANPARÁ

1. INTRODUÇÃO

A Política de Segurança tem por finalidade fundamentar as normas e procedimentos de segurança implementados pelo BANPARÁ.

2. OBJETIVO

A Política de Segurança do BANPARÁ possui como objetivos específicos:

2.1 - Orientar, por meio de suas diretrizes, as ações de segurança, para reduzir riscos e garantir níveis aceitáveis de segurança pessoal (capital humano), física (ativo patrimonial) e lógica (bens de informação);

2.2 - Definir um conjunto de medidas que assegure proteção ao capital humano, ao ativo patrimonial e aos bens de informação onde a organização se fizer presente;

2.3 - Estabelecer um conjunto de recomendações que assegure a integridade e a confidencialidade dos bens de informação gerados e utilizados no Banco, objetivando a proteção desses bens às ameaças, minimizando os danos, maximizando o retorno dos investimentos e garantindo a continuidade dos negócios;

2.4 - Definir e manter atualizado o Plano de Continuidade de Negócios, Plano de Recuperação de desastres e Plano de resposta a incidentes, a serem elaborados por equipe multidisciplinar, para ocorrências que possam alterar, ameaçar ou interromper as atividades do Banco.

3. DEFINIÇÕES

3.1 – Capital humano:

São todas as pessoas que, direta ou indiretamente, estão envolvidas na consecução do objeto fim da instituição.

3.2 - Bens Patrimoniais:

São todas as instalações físicas, internas e externas, onde a organização se fizer presente.

3.3 - Bens de Informação:

São todas as informações utilizadas no Banco para a realização de seus negócios, os meios utilizados para suportar essas informações e os recursos necessários para acessar essas informações.

3.4 - Proteção e Confiabilidade:

O bem de informação é considerado protegido e confiável quando apresentar simultaneamente as seguintes características e, se indevidamente divulgado ou utilizado, expor o Banco a danos materiais, legais e de imagem:

3.4.1 - Integridade: É exato e completo.

3.4.2 - Confidencialidade: É acessível somente às pessoas autorizadas.

3.4.3 - Disponibilidade: É acessível sempre que necessário.

4. POLÍTICAS

4.1. Segurança de Pessoal:

4.1.1 - Definir critérios de aperfeiçoamento do processo de seleção de funcionários, visando a admissão de profissionais que não representem riscos à segurança do Banco;

4.1.2 - Planejar treinamentos periódicos para reciclagem e capacitação dos funcionários, mantendo-os atualizados quanto às políticas e diretrizes de segurança de pessoal, patrimonial e lógica;

4.1.3 - Definir mecanismos securitários para o quadro funcional;

4.1.4 - Definir critérios para a formação de equipe multidisciplinar responsável pela elaboração do plano de continuidade de negócios;

4.1.5 - Definir plano de segurança para proteção dos funcionários e dos dirigentes do Banco, inclusive quando em viagem à serviço;

4.1.6 - Elaborar e manter atualizados os manuais de segurança de pessoal, definindo responsabilidades e atribuições específicas para os funcionários e colaboradores.

4.2 - Segurança Patrimonial:

4.2.1 - Definir mecanismos para manutenção e proteção das instalações

elétricas/eletrônicas nas unidades do Banco;

4.2.2 - Criar normas e procedimentos de segurança para melhorar a gestão da contratação de terceiros;

4.2.3 - Criar normas e procedimentos específicos que envolvam a plena conservação de suas instalações e edificações;

4.2.4 - Definir mecanismos securitários para cobertura de seu patrimônio;

4.2.5 - Definir mecanismos para garantir que, na alienação ou reutilização de equipamentos, haja remoção das informações classificadas como confidenciais e/ou restritas;

4.2.6 - Criar normas e procedimentos para o descarte de materiais;

4.2.7 - Criar e manter sistema de combate a incêndio em todas as dependências da Instituição;

4.2.8 - Definir sistema de controle de acesso físico capaz de evitar/prevenir perdas materiais, tais como: furtos, roubos, atos de espionagem, sabotagem;

4.2.9 - Definir padronização para segurança patrimonial (muros altos, cerca elétrica, grades, entrada única, etc) em todas as unidades, de modo a evitar acessos indevidos;

4.2.10 – Determinar que os projetos de instalação de novos pontos de atendimento e de reformas atendam os requisitos de segurança vigentes;

4.2.11 – Determinar que nos planos de segurança das unidades do Banco seja contemplado o número mínimo de equipamentos de segurança exigidos em normativos legais e definido pela área de Segurança;

4.2.12 - Definir normas e procedimentos para proteção do meio ambiente natural, no que se refere à conservação das áreas internas e circunvizinhas das unidades;

4.2.13 - Elaborar e manter atualizados o manual de segurança patrimonial, definindo responsabilidades e atribuições específicas para os funcionários e colaboradores;

4.2.14 – Estabelecer normas e procedimentos de auditoria patrimonial para todas as unidades visando garantir o acompanhamento e o cumprimento das políticas;

4.3 - Segurança Lógica:

4.3.1 - Criar e manter a sistemática de segurança da informação visando assegurar a confidencialidade, a integridade e a disponibilidade dos bens de informação;

4.3.2 – Estabelecer normas para a utilização dos meios de comunicação disponibilizados pelo Banco;

4.3.3 - Definir critérios que permitam a classificação dos bens de informação do Banco quanto à sensibilidade e criticidade;

4.3.4 - Definir processos de identificação, avaliação e mitigação de riscos aos ativos de Informação;

4.3.5 - Definir a segregação dos ambientes computacionais do Banco;

4.3.6 - Elaborar e manter atualizado o manual de segurança da informação, definindo responsabilidades e atribuições específicas para os funcionários e colaboradores;

4.3.7 - Definir normas e procedimentos de segurança para o desenvolvimento, aquisição, homologação e manutenção de sistemas;

4.3.8 - Definir normas e procedimentos de controle de acesso a todos os sistemas corporativos, para a rede interna e acessos remotos;

4.3.9 - Definir normas e procedimentos para a elaboração do inventário de todos os ativos de tecnologia da informação;

4.3.10 - Definir normas e procedimentos de auditoria de sistema visando o cumprimento das Políticas;

4.3.12 - Designar os gestores para gerenciar os aplicativos e sistemas utilizados no Banco;

4.3.13- Definir e implantar Termo de Confidencialidade, Zelo e de Responsabilidade sobre os bens de informações do Banco, que deverá ser assinado por todos os diretores, empregados, estagiários e contratados que, de alguma forma, tenham acesso a essas informações.

4.3.14 - Definir normas e procedimentos para a aquisição, controle e uso dos certificados digitais do Banco;

4.3.15 - Definir normas e procedimentos para controle e utilização de chaves criptográficas e senhas dos sistemas e aplicativos;

4.3.16 - Definir normas e procedimentos de segurança da Rede Corporativa e infra-estrutura;

4.3.17 - Definir normas e procedimentos de retenção e destruição de dados;

4.3.18 - Definir normas e procedimentos de segurança para o transporte e armazenamento de mídias;

5. DAS RESPONSABILIDADES

Caberá ao COMITÊ DE SEGURANÇA FÍSICA E LÓGICA, sob convocação de seu coordenador, titular da Superintendência de Segurança de Tecnologia da Informação – SUSIN, a manutenção, revisão e atualização desta Política de Segurança, e ao Núcleo de Auditoria – NUAUD a apuração de responsabilidade pelo seu descumprimento.

6. CONSIDERAÇÕES FINAIS

A Política de Segurança deverá ser amplamente divulgada a todo o funcionalismo do BANPARÁ, diretores, estagiários e contratados e o seu acesso disponibilizado nos canais internos de comunicação.

Pelo descumprimento das normas e procedimentos constantes das políticas de segurança, má utilização ou danos causados aos bens de informação e patrimoniais, intencionais ou não, responderão administrativamente, sem prejuízo de ação civil e penal cabíveis, os diretores, empregados, estagiários e contratados.

ANEXO III

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 2011.

_____

Assinatura do contratado

ANEXO IV

TERMO DE ACEITE DE ATIVIDADE

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**

ANEXO V

ATESTADO DE EXPERIÊNCIA NA PRESTAÇÃO DE SERVIÇOS DE PORTE COMPATÍVEL COM O OBJETO DESTE EDITAL

Referência: **PREGÃO XX/2011 - BANPARÁ**
Data: _____
Empresa Licitante: _____
CNPJ: _____

ATESTAMOS, para fins de comprovação junto ao Banco do estado do Pará - Banpará, que a empresa acima referida executou ou vem executando serviços de diagnóstico e gerenciamento continuado em segurança de tecnologia da informação, contemplando: implantação, treinamento, administração, gerenciamento e monitoração remota 24x7(vinte e quatro horas por dia, sete dias na semana) do serviço de Firewall/VPN,IPS, Gestão de Vulnerabilidades, Filtro de E-mail, Gestão de Antivírus Corporativo e consultorias em segurança da informação, utilizando *appliances* em comodato, enquanto durar o contrato, para no mínimo 2.000 (dois mil) hosts, no período transcorrido entre *(data inicial, em dd/mm/aa)* e *(data final, em dd/mm/aa)*.
ATESTAMOS, ainda, que os serviços foram/vêm sendo prestados de forma satisfatória, não havendo em nossos registros nenhum fato que desabone sua conduta e responsabilidade em relação às tarefas assumidas.

(*Localidade*), (*dia)* de (*mês*) de 2011.

Representante da Empresa Atestante:

_____
Nome: .....
Cargo / Função: .....
CPF: .....Telefone:.....
E-mail: .....
Documento de Identidade (número,data,emissor): .....

OBS.:

a) Este atestado deve ser emitido em papel timbrado da Empresa Atestante.
b) Deve ser apresentado apenas um atestado por Empresa Atestante.

ANEXO VI (MODELO DE PROPOSTA DE PREÇOS)

PREGÃO ELETRÔNICO Nº /2011 - BANCO DO ESTADO DO PARÁ S/A

Ao Banco do Estado do Pará

11	**TOTAL GERAL do contrato para 36 meses (TOTAL 1 + TOTAL 2 + TOTAL 3 + Total 4)**				

Comissão de Licitação
Processo Nr: _____
Edital Nr: _____

A empresa _____, CNPJ _____, apresenta a seguir seus preços parcial e global para execução dos serviços, a qual é no importe de R$ xxxxxxxx, referente CONTRATAÇÃO DE EMPRESA ESPECIALIZADA NA PRESTAÇÃO DE SERVIÇOS GERENCIADOS DE SEGURANÇA LÓGICA.

O prazo de validade da proposta de preços é de .....dias **consecutivos**, contados da data da abertura da licitação. (no mínimo 120 dias).

Prazo de Vigência do Contrato de 12 (doze) meses, contados a partir de sua assinatura.

Declaramos que os serviços serão prestados 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 instrumento de 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. /2011.

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, **NOS COMPROMETEMOS A REALIZAR A REFERIDA ABERTURA DA CONTA NO PRAZO MÁXIMO DE ATÉ 05 (CINCO DIAS) CONSECUTIVOS CONTADOS DA**

PUBLICAÇÃO NA IMPRENSA OFICIAL DO ESTADO DO PARÁ D A HOMOLOGAÇÃO DO RESULTADO FINAL DA LICITAÇÃO.

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 Anexo1 deste edital, prevalecerão as últimas.

Item	Descrição	Qtd	Instalação (R$)	Unit	Total 36 Meses (R$)
01	Serviço de Firewall/VPN, fornecido com (02) equipamentos em Ativo-Ativo;	1			
02	Serviço de IPS (Sistema de Prevenção de Intrusos) fornecido com, no mínimo, 02 (dois) equipamento sensor fail-open e 01 (um) equipamento para gerência	1			
03	Serviço de Gestão de Vulnerabilidades fornecido, no mínimo, com 01 (um) equipamento com suporte para varredura em até 2500 (duas mil quinhentos) endereços IP;	1			
04	Serviço de Filtro de E-mail fornecido com, no mínimo, 02 (dois) equipamentos redundantes para 2.000 (duas mil) caixas postais.	1			
05	Serviço de Gestão de Antivírus Corporativo para 2500 dispositivos	1			
06	TOTAL PARCIAL		Total 1		TOTAL 2
Item	Descrição	Qtd.	-	Unit.	Total Horas (R$)
09	Banco de horas técnicas	6000			
10	TOTAL PARCIAL 2				TOTAL 3
Item	TREINAMENTOS NÃO OFICIAIS	Carga	Valor		
01	Serviço de Firewall/VPN				
02	Serviço de IPS				
03	Serviço de Gestão de Vulnerabilidades				
04	Serviço de Filtro de E-mail				
05	Serviço de Gestão de Antivírus Corporativo				
06	Total Parcial		Total 4		

ANEXO VII

DECLARAÇÃO DE INEXISTÊNCIA DE FATO IMPEDITIVO À HABILITAÇÃO

(Modelo)

[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

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.

ANEXO X

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 VI

DECLARAÇÃO DE QUE ESTÁ DE ACORDO COM A REALIZAÇÃO DOS SERVIÇOS

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 NÃO COMPARECEU A VISITA TÉCNICA REALIZADA NAS 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, entretanto ESTÁ DE ACORDO COM A REALIZAÇÃO DOS SERVIÇOS, NÃO TENDO NENHUMA DÚVIDA QUE VENHA A MODIFICAR OS QUANTITATIVOS E ESPECIFICAÇÕES INDICADAS NO TERMO DE REFERÊNCIA E DEMAIS ANEXOS o Edital.

Belém-Pará.....de.....2011

_____

Nome e assinatura da pessoa com poderes para fazer a declaração

ANEXO IX – MINUTA DE CONTRATO

INSTRUMENTO PARTICULAR DE CONTRATO DE CONTRATAÇÃO DE EMPRESA ESPECIALIZADA NA PRESTAÇÃO DE SERVIÇOS GERENCIADOS DE SEGURANÇA LÓGICA, QUE FAZEM ENTRE SI O BANCO DO ESTADO DO PARÁ S/A. E A EMPRESA _____, 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 n.º 04.913.711/0001-08, neste ato representado pelo seu Presidente _____ (qualificação) e sua Diretora _____ (qualificação), ambos residentes e domiciliados nesta cidade, doravante designado **CONTRATANTE** e, de outro lado, a empresa _____, sediada na cidade de _____, sito travessa à _____, nº _____, Bairro _____, CEP: _____, inscrita no C.N.P.J. nº _____, denominada **CONTRATADA**, neste ato representado por _____, (qualificação) portador do RG nº _____, CPF/MF nº _____, residente e domiciliado na cidade de _____, (endereço completo), Bairro _____, CEP _____, celebram o presente Contrato, por Licitação na modalidade **Pregão Eletrônico Nº _____**, na forma da Lei Federal Nº 10.520/2002, Lei Estadual nº 6.474/2002 e Decreto Estadual nº 0199/2003 e, subsidiariamente, Lei nº 8.666/93 e suas alterações posteriores, conforme o Processo nº 2300/2010 – SUSIN, segundo as cláusulas e condições a seguir:

CLÁUSULA PRIMEIRA - DO OBJETO

O objeto do presente contrato é a CONTRATAÇÃO DE EMPRESA ESPECIALIZADA NA PRESTAÇÃO DE SERVIÇOS GERENCIADOS DE SEGURANÇA LÓGICA, NO MODELO 24HS POR DIA, 7 DIAS POR SEMANA, 365 DIAS POR ANO, INICIALMENTE POR 36 MESES, INCLUINDO O CONJUNTO DE HARDWARE E SOFTWARE FORNECIDOS EM REGIME DE COMODATO, NECESSÁRIOS E SUFICIENTES PARA A PRESTAÇÃO DESSES SERVIÇOS CONFORME ESCOPO ABAIXO, em conformidade com as especificações técnicas contidas no Anexo I do Edital n° xxxxx e na Proposta de Preços Nº xxxx, as quais fazem parte integrante deste contrato.

- Serviço de Firewall/VPN, para controle do tráfego nos segmentos protegidos;
- Serviço de IPS (Sistema de Prevenção de Intrusos), para detecção e bloqueio de intrusão nos segmentos protegidos;
- Serviço de Gestão de Vulnerabilidades, para descoberta e gestão de eventuais de falhas segurança no ambiente;

- Serviço de Filtro de E-mail, para controle do tráfego de e-mail e proteção contra vírus, spam e conteúdo indesejado;
- Serviço de Gestão de Antivírus Corporativo para os servidores e estações de trabalho do BANPARÁ para identificar e mitigar infecções por vírus;
- Disponibilização de banco de até 6.000 (seis mil) horas para a prestação de serviços técnicos, que possam ser utilizadas sob demanda.

PARÁGRAFO ÚNICO: O fornecimento e a prestação de serviço será fiscalizado, conforme o caso, por um funcionário designado pelo **CONTRATANTE**, com autoridade para exercer tal função.

CLÁUSULA SEGUNDA – DAS OBRIGAÇÕES DA CONTRATADA
Para o fiel cumprimento deste contrato, a **CONTRATADA** se obriga a:

a) Dar integral cumprimento ao Termo de Referência, em especial as obrigações previstas no item 15, 3.2.1, 3.2.2, 3.2.3 e 3.24 do Termo de Referência – Anexo I do edital, à Legislação vigente, a todas as normas vigentes, à sua proposta, bem como às necessidades e orientações do BANPARÁ;

b) Usar pessoal próprio, contratado sob inteira responsabilidade, para, sob a sua supervisão direta prestar o serviço. Para tanto, recrutar os trabalhadores necessários, arcando com todos os encargos decorrentes da contratação;

c) Acatar todas as exigências do **CONTRATANTE**, sujeitando-se à ampla e irrestrita fiscalização, prestando todos os esclarecimentos solicitados e atendendo às reclamações formuladas;

d) 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**;

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) 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;

g) 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.

h) Reembolsar o **CONTRATANTE** de todas as despesas que este tiver decorrentes de:

i) Reconhecimento judicial de titularidade de vínculo empregatício de prepostos seus com ao **CONTRATANTE**, ou qualquer empresa do mesmo grupo econômico;
ii) Reconhecimento judicial de solidariedade ou subsidiariedade do **CONTRATANTE** ou qualquer outra empresa do mesmo grupo econômico no cumprimento das obrigações previdenciárias da **CONTRATADA**.

i) 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**, individual ou coletivamente, no pólo passivo da eventual reclamação trabalhista.

j) Prestar garantia na forma estabelecida neste Contrato;

k) 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**;

l) 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;

m) Não subcontratar, no todo ou em parte, sem prévia anuência do **CONTRATANTE**.

n) Arcar com as despesas decorrentes da prestação dos serviços objeto do presente instrumento contratual.

o) Observar os requisitos previstos no Termo de Referência – Anexo I do Edital.

p) Observar a Política de Segurança do BANPARÁ – Anexo II do Edital.

q) Observar o Acordo de Nível de Serviço – SLA previsto no item 04 do Termo de Referência – Anexo I do Edital, bem como o item 18, quanto a Avaliação do Desempenho e Qualidade do Serviço.

r) Emitir Nota Fiscal Eletrônica – Nfe, modelo 55, nos termos do Protocolo ICMS 42/2009 de 03 de julho de 2009.

s) Cumprir integralmente as condições de implantação dos serviços, na forma do item 10 do Termo de Referência – Anexo I do Edital.

PARÁGRAFO ÚNICO: A responsabilidade da **CONTRATADA** pela prestação de serviço global, 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
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, através da Superintendência de Segurança da Informação - SUSIN, atestando ao final sua prestação, se, e somente se, os serviços executados atenderem plenamente às especificações constantes do Termo de Referência;

c) efetivar a satisfação do crédito da **CONTRATADA**, nos precisos termos dispostos no Contrato;

d) Prestar as informações e os esclarecimentos que venham a ser solicitados pela **CONTRATADA**;

e) Efetuar o pagamento na forma convencionada;

f) 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;

g) Acompanhar e fiscalizar a prestação dos serviços por meio de servidor indicado e designado como seu representante.

h) Cumprir as obrigações definidas no termo de referência, em especial no item 16.

i) Caso ocorra o desligamento de qualquer um dos profissionais exigidos no item 3.2.5 ou 3.2.5.1 do Termo de Referência, durante a vigência do contrato, a empresa deverá providenciar um substituto, com as mesmas certificações, no prazo máximo de 15 dias.

CLÁUSULA QUARTA: DA INEXISTÊNCIA DE VÍNCULO EMPREGATÍCIO
Fica desde já entendido que os profissionais 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 QUINTA - DOS PREÇOS E CONDIÇÕES DE PAGAMENTO
O valor global deste contrato é de **R$- ____ (extenso)**, conforme abaixo especificado:

Item	Descrição	Qtd	Instalação (R$)	Unit	Total 36 Meses (R$)
01	Serviço de Firewall/VPN, fornecido com (02) equipamentos em Ativo-Ativo;	1			
02	Serviço de IPS (Sistema de Prevenção de Intrusos) fornecido com, no mínimo, 02 (dois) equipamento sensor fail-open e 01 (um) equipamento para gerência	1			
03	Serviço de Gestão de Vulnerabilidades fornecido, no mínimo, com 01 (um) equipamento com suporte para varredura em até 2500 (duas mil quinhentos) endereços IP;	1			
04	Serviço de Filtro de E-mail fornecido com, no mínimo, 02 (dois) equipamentos redundantes para 2.000 (duas mil) caixas postais.	1			
05	Serviço de Gestão de Antivírus Corporativo para 2500 dispositivos	1			
06	TOTAL PARCIAL		Total 1		TOTAL 2
Item	Descrição	Qtd.	-	Unit.	Total Horas (R$)
09	Banco de horas técnicas	6000			
10	TOTAL PARCIAL 2				TOTAL 3
Item	TREINAMENTOS NÃO OFICIAIS	Carga	Valor		
01	Serviço de Firewall/VPN				
02	Serviço de IPS				
03	Serviço de Gestão de Vulnerabilidades				
04	Serviço de Filtro de E-mail				
05	Serviço de Gestão de Antivírus Corporativo				
06	Total Parcial		Total 4		
11	TOTAL GERAL do contrato para 36 meses (TOTAL 1 + TOTAL 2 + TOTAL 3 + Total 4)				

PARÁGRAFO PRIMEIRO: O pagamento será realizado conforme item 13 do Termo de Referência – Anexo I do Edital.

PARÁGRAFO SEGUNDO: A realização do pagamento de que trata o item acima fica condicionada a apresentação dos documentos, caso os anteriormente apresentados estejam vencidos: 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 do licitante.

PARÁGRAFO TERCEIRO: No preço 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, e outros, ficando excluída qualquer solidariedade do CONTRATANTE, por eventuais autuações.

PARÁGRAFO QUARTO: As despesas decorrentes da implementação dos serviços, objeto deste contrato, deverão ser arcadas pela CONTRATADA.

PARÁGRAFO QUINTO: A devolução de notas/faturas não servirá de pretexto para a suspensão dos serviços ou ao descumprimento de cláusulas contratuais.

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: 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 OITAVO: No preço referido no *caput* desta cláusula já estão inclusos todos os tributos, contribuições e demais encargos que incidam ou venham a incidir nesta prestação do serviço, os quais são de exclusiva responsabilidade da **CONTRATADA**.

PARÁGRAFO NONO: Os pagamentos a serem efetuados por parte do **CONTRATANTE** somente serão realizados após a homologação dos serviços pela área responsável (SUSIN), para a liquidação do pagamento.

PARÁGRAFO DEZ: Será efetuada a retenção na fonte de todos os tributos e contribuições exigidos pela legislação em vigor, para a prestação de serviço, objeto deste contrato.

PARÁGRAFO ONZE: O **CONTRATANTE** não assumirá responsabilidade alguma pelo pagamento de tributos e encargos que competirem à **CONTRATADA**, nem se obrigará a restituir-lhes valores, principais ou acessórios, que esta, porventura, despender com pagamentos dessa natureza.

PARÁGRAFO DOZE: 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.

CLÁUSULA SEXTA: **DA APRESENTAÇÃO DE DOCUMENTOS PARA PAGAMENTO**
Os pagamentos dos serviços prestados ficarão condicionados, a critério do **CONTRATANTE**, à apresentação, pela **CONTRATADA**, dos seguintes documentos, no original ou cópia autenticada:

a) Comprovantes dos recolhimentos previdenciários;

b) Comprovantes dos depósitos do FGTS, realizados na conta vinculada dos empregados da empresa.

PARÁGRAFO PRIMEIRO: 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.

PARÁGRAFO SEGUNDO: O descumprimento do disposto nesta cláusula faculta ao **CONTRATANTE** o direito de reter o valor correspondente ao pagamento dos serviços até a regularização da pendência.

CLÁUSULA SÉTIMA - DA VIGÊNCIA
O presente contrato tem um prazo de vigência de 36 (trinta) meses, a contar da data da assinatura do mesmo, podendo ser prorrogado nos termos do disposto na Lei nº. 8.666/93.

CLÁUSULA OITAVA – 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 será prestado conforme abaixo:

a) Em se tratando de caução: 5% do valor global do contrato que será creditado em conta de poupança vinculada ao contrato nº. /2011, aberta na agência Belém Centro, 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: 5% do valor global do contrato, em qualquer Instituição Financeira Oficial a critério da **CONTRATADA**;

c) Em se tratando de seguro garantia: em qualquer seguradora, a critério da **CONTRATADA**, no valor correspondente a 5% do valor do contrato.

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, fica a **CONTRATADA** obrigada a complementar o valor da garantia de modo a corresponder sempre a 5% (cinco por cento) do valor do contrato.

CLÁUSULA NONA - 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 2 (dois) 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;

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: A multa moratória poderá ser cobrada pelo atraso injustificado no cumprimento do objeto ou de prazos estipulados, nos seguintes percentuais:

a) 5% (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:

a.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;

a.2) Cumprir fielmente as cláusulas contratuais;

a.3) Responder pelos encargos fiscais e comerciais resultantes da adjudicação desta licitação;

a.4) 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;
a.5) 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.

b) nos demais casos não regulados por este instrumento contratual, prevalece as disposições do item 14 do Termo de Referencia (anexo a este).

PARÁGRAFO TERCEIRO: A multa por inexecução contratual poderá ser aplicada nos seguintes percentuais e situações:

a) 10% (dez por cento) pela inexecução parcial do contrato, calculada sobre o valor global do contrato;
b) 15% (quinze por cento) pela inexecução total do contrato, calculada sobre o valor global do contrato;

PARÁGRAFO QUARTO: No caso rescisão por falta imputada à **CONTRATADA**, será aplicada multa de 30% (trinta por cento) do valor global do contrato.

PARÁGRAFO QUINTO: O **CONTRATANTE** poderá aplicar, cumulativamente, à **CONTRATADA** multa moratória e multa por inexecução deste ajuste.

PARÁGRAFO SEXTO: As multas poderão ser aplicadas cumulativamente com as sanções de advertência, suspensão temporária ou declaração de inidoneidade.

PARÁGRAFO SÉTIMO: A aplicação das multas aludidas nesta cláusula não obsta que o **CONTRATANTE** rescinda unilateralmente o contrato e aplique as demais sanções.

PARÁGRAFO OITAVO: A critério do **CONTRATANTE**, as multas poderão ser deduzidas dos pagamentos devidos à **CONTRATADA**, independentemente de comunicação ou interpelação judicial, sem prejuízo da cobrança judicial no caso de insuficiência dos referidos valores.

PARÁGRAFO NONO: No caso de aplicação de multa moratória, considerar-se-á, como intimação do ato, o recebimento, pela empresa, da comunicação respectiva, por correspondência.

PARÁGRAFO DEZ: 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 ou multa, na forma do que dispõem os parágrafos primeiro e segundo da presente cláusula deste contrato.

b) por dois anos:

i) não conclusão dos serviços contratados;

ii) prestação do serviço em desacordo com o termo de referência, 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 quando fizer qualquer 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 deste contrato;

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 deste contrato, sem consentimento prévio do **CONTRATANTE**.

PARÁGRAFO ONZE: 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 DOZE: A CONTRATADA/ADJUDICATÁRIA que, convocada dentro do prazo de validade de sua Proposta, não assinar o Contrato, deixar de entregar documentação exigida no Edital, apresentar documentação falsa, ensejar o retardamento da execução de seu objeto, não mantiver a Proposta, falhar ou fraudar na execução do Contrato, comportar-se de modo inidôneo, fizer declaração falsa ou cometer fraude fiscal, garantido o direito à ampla defesa, ficará impedida de licitar e de contratar com a União, Estados, Distrito Federal ou Município, e será descredenciada no SICAF, pelo prazo de até 05 (cinco) anos, sem prejuízo das multas previstas no Edital e no Contrato e das demais cominações legais;

PARÁGRAFO TREZE: Após a conclusão do processo administrativo, garantida ampla defesa, serão devolvidos os valores retidos na forma do parágrafo oitavo, corrigidos pelo índice da poupança, caso o julgamento seja favorável à **CONTRATADA**.

PARÁGRAFO QUATORZE: 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 QUINZE: 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 DEZ - 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, sem prejuízo das responsabilidades civil e penal cabíveis, inclusive o disposto na **Cláusula Nona**;
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.

CLÁUSULA DOZE – DO FORO

Fica eleito o Foro da Comarca de Belém do Pará, para dirimir controvérsias oriundas do presente contrato, renunciando a qualquer outro, por mais privilegiado que o seja.

E assim, por estarem juntos e contratados, assinam o presente instrumento em 02 (duas) vias de igual teor e forma, subscritas pelas testemunhas abaixo qualificadas, para que produza seus efeitos jurídicos.

Belém (PA), de de 2011.

BANCO DO ESTADO DO PARÁ S. A.

CONTRATADA

TESTEMUNHAS:

NOME:	**NOME:**
CPF:	**CPF:**