CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO

CONTRATO CNMP Nº 31/2016

CONTRATO QUE ENTRE SI CELEBRAM A UNIÃO, POR INTERMÉDIO DO CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO – CNMP, E A PESSOA JURÍDICA NCT INFORMÁTICA LTDA, NA FORMA ABAIXO:

A UNIÃO, por intermédio do **CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO**, CNPJ n.º 11.439.520/0001-11, situado no Setor de Administração Federal Sul - SAFS, quadra 02, lote 03, Edifício Adail Belmonte, Brasília/DF, representado neste ato por seu Ordenador de Despesas, Sr. **ROBERTO FUÍNA VERSIANI**, brasileiro, servidor público, RG 441.122 – SSP/MA, CPF: 332.472.691-34, no uso da competência que lhe foi atribuída pela Portaria CNMP-SG n.º 119, de 31 de maio de 2016, ou, nas ausências e impedimentos desta, pelo seu substituto, Sr. **HUMBERTO DE CAMPOS COSTA**, brasileiro, servidor público, RG: 1.229.850 – SSP/DF, CPF: 602.710.781-20, conforme Portaria CNMP-SG nº 119, de 31 de maio de 2016, ambos residentes e domiciliados nesta Capital, doravante denominado simplesmente **CONTRATANTE** e a pessoa jurídica **NCT INFORMÁTICA LTDA**, CNPJ n.º 03.017.428/0001-35, estabelecida no Setor Bancário Sul – SBS, Quadra 2, Lote 3, Bloco Q, 8º andar, Sala 801, Centro Empresarial João Carlos Saad, Asa Sul, Brasília/DF, CEP 70070-120, neste ato representada por **PRISCILA KIN YAMAMOTO JORANHEZON**, brasileira, casada, inscrita no RG sob o nº 2.373.366 SSP/DF, e no CPF sob o nº 022.373.811-51, residente e domiciliada em Brasília/DF, e daqui por diante designada simplesmente **CONTRATADA**, tendo em vista o contido no Processo CNMP n.º 0.00.002.000597/2014-86, referente ao Pregão Eletrônico CNMP nº 16/2016, considerando as disposições estabelecidas na Lei nº 8.666/1993, Lei nº 10.520/2002 e, ainda, pelos Decreto nº 3.555/2000, Decreto nº 5.450/2005, pela Lei Complementar nº 123/2006, Decreto nº 2.271, de 07/07/97, e I.N SLTI/MPOG nº 2/2008, e demais normas pertinentes, têm entre si, justo e avençado, e celebram o presente Contrato, mediante as seguintes cláusulas e condições:

CLÁUSULA PRIMEIRA – DO OBJETO

O presente Contrato tem por objeto a prestação de serviço de proteção, controle e resposta a incidentes de rede, monitoração dos serviços de filtro de pacote, controle de aplicação, administração de largura de banda, QoS, suporte para conexões VPN IPSec e SSL, IPS, prevenção contra ameaças de vírus,

spywares e malwares Zero Day, filtro de URL, controle de transmissão de dados e acesso à internet com uso de solução, do tipo appliance, com características de Next Generation Firewall (NGFW), fazendo parte do serviço o fornecimento, a instalação, configuração de hardware e softwares da solução, para o Conselho Nacional do Ministério Público – CNMP, situado no Setor de Administração Federal Sul – SAFS, Quadra 02, Lote 03, Edifício Adail Belmonte, Brasília – DF.

Parágrafo único. A prestação dos serviços obedecerá ao estipulado neste contrato, bem como, às obrigações assumidas nos documentos adiante enumerados constantes do Processo nº 0.00.002.000597/2016-86, e que independentemente de transcrição, fazem parte integrante e complementar deste contrato, no que não o contrariem:

a) Edital de Pregão nº 16/2016;

b) Ata da Sessão do Pregão, datada de 26/07/2016;

c) Proposta final firmada pela CONTRATADA em 25/07/2016, contendo o valor global e unitário dos serviços a serem executados.

CLÁUSULA SEGUNDA – DO REGIME DE EXECUÇÃO

A forma de execução do presente Contrato será indireta, sob o regime de empreitada por preço global, conforme disposto na Lei nº 8.666/1993.

CLÁUSULA TERCEIRA – DAS OBRIGAÇÕES DO CONTRATANTE

Constituem obrigações do CONTRATANTE, sem prejuízo das disposições específicas estabelecidas do Edital e ou do Termo de Referência:

1) Cumprir e fazer cumprir o disposto neste Contrato;

2) Relacionar-se com a CONTRATADA exclusivamente por meio de pessoa por ela indicada;

3) Assegurar o livre acesso dos empregados da CONTRATADA, quando devidamente identificados e uniformizados, aos locais em que devam executar suas tarefas;

4) Efetuar, com pontualidade, os pagamentos à CONTRATADA, após o cumprimento das formalidades legais;

5) Fornecer à CONTRATADA, todos os esclarecimentos necessários para execução dos serviços e demais informações que estes venham a solicitar para o desempenho dos serviços ora contratados.

Parágrafo Primeiro – O CONTRATANTE reserva para si o direito de aplicar sanções ou rescindir o contrato, no caso de inobservância pela CONTRATADA de quaisquer das cláusulas e condições estabelecidas neste Contrato.

Parágrafo Segundo – O CONTRATANTE efetuará a fiscalização e o acompanhamento da execução dos serviços por meio do Gestor/Fiscal do Contrato, devendo este fazer anotações e registros de todas as ocorrências e determinar o que for necessário à regularização das falhas ou defeitos observados.

CLÁUSULA QUARTA – DAS OBRIGAÇÕES DA CONTRATADA

A CONTRATADA se obriga a cumprir fielmente o estipulado no presente instrumento, bem como as obrigações específicas estabelecidas do Edital e ou do Termo de Referência e, ainda, em especial:

1) Executar os serviços contratados em conformidade com o Termo de Referência – Anexo I do Edital, o qual fornece todas as orientações do CONTRATANTE;

2) Prestar todos os esclarecimentos que lhe forem solicitados pelo CONTRATANTE, atendendo prontamente a todas as reclamações;

3) Relacionar-se com o CONTRATANTE, exclusivamente, por meio do Gestor/Fiscal do Contrato;

4) Indicar, formalmente, preposto devidamente credenciado, visando a estabelecer contatos com o representante do CONTRATANTE durante a vigência do Contrato;

5) Cumprir todas as orientações do CONTRATANTE para o fiel desempenho das atividades especificadas e sujeitar-se a mais ampla e irrestrita fiscalização, prestando todos os esclarecimentos que lhe forem solicitados e atendendo às reclamações formuladas;

6) Manter, quando nas dependências do CONTRATANTE, os empregados devidamente identificados, por meio de crachás, e uniformizados de maneira condizente com o serviço a executar, quando necessário, observando, ainda, as normas internas e de segurança;

7) Responsabilizar-se pelas despesas com todos encargos e obrigações sociais, trabalhistas e fiscais de seus empregados, os quais não terão, em hipótese alguma, qualquer relação de emprego com o CONTRATANTE;

8) O atraso na apresentação, por parte da empresa, da fatura ou dos documentos exigidos como condição para pagamento importará em prorrogação automática do prazo em igual número de dia de vencimento da obrigação do CONTRATANTE;

9) Não transferir a outrem, no todo ou em parte, o objeto do Contrato, **sem prévia e expressa anuência do CONTRATANTE;**

10) Não caucionar ou utilizar o Contrato para qualquer operação financeira, sob pena de rescisão contratual;

11) Manter durante a vigência do Contrato todas as condições de habilitação e qualificação exigidas na licitação;

12) Disponibilizar uma conta *e-mail* para fins de comunicação entre as partes, e manter atualizados o endereço comercial e os números de telefone e de fax;

13) Comunicar, por escrito, eventual atraso ou paralisação dos serviços, apresentando razões justificadoras a serem apreciadas pelo CONTRATANTE;

14) Manter sigilo, sob pena de responsabilidade, sobre todo e qualquer assunto de interesse do CONTRATANTE ou de terceiros de que tomar conhecimento em razão da execução dos serviços, devendo orientar seus empregados nesse sentido;

15) Não reproduzir, divulgar ou utilizar em benefício próprio, ou de terceiros, quaisquer informações de que tenha tomado ciência em razão da execução dos serviços discriminados, sem o consentimento, prévio e por escrito, do CONTRATANTE;

16) Não utilizar o nome do CONTRATANTE, ou sua qualidade de CONTRATADA, em quaisquer atividades de divulgação empresarial, como, por exemplo, em cartões de visita, anúncios e impressos, sob pena de rescisão do presente Contrato;

17) Responsabilizar-se por todo e qualquer acidente do trabalho, dano ou prejuízo causado ao patrimônio do CONTRATANTE ou de terceiros, decorrente da execução do serviço contratado;

18) Apresentar os documentos fiscais de cobrança em conformidade com o estabelecido neste Contrato.

CLÁUSULA QUINTA – DO PRAZO DE VIGÊNCIA

O presente contrato terá vigência de 60 meses, contados a partir de sua assinatura.

CLÁUSULA SEXTA – DO VALOR

O valor mensal estimado dos serviços ora contratados é de R$ 11.653,33 (onze mil, seiscentos e cinquenta e três reais e trinta e três centavos), perfazendo um total global de R$ 699.199,80 (seiscentos e noventa e nove mil, cento e noventa e nove reais e oitenta centavos), durante a vigência deste Contrato, conforme quadro abaixo:

Descrição	Valor Mensal
Solução de Segurança	R$ 11.653,33
Valor Global da Solução (Valor Mensal x 60)	**R$ 699.199,80**

CLÁUSULA SÉTIMA – DO PAGAMENTO

O pagamento será efetuado conforme o item 10 do Termo de Referência, Anexo I do Edital.

Parágrafo primeiro. Para execução do pagamento de que trata a presente Cláusula, a CONTRATADA deverá fazer constar como beneficiário/cliente, da Nota Fiscal/Fatura correspondente, emitida sem rasuras, o **CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO, CNPJ nº 11.439.520/0001-11,** e ainda, o número da Nota de Empenho, os números do Banco, da Agência e da conta-corrente da CONTRATADA e a descrição clara e sucinta do objeto.

Parágrafo segundo. Sobre o valor da Nota Fiscal, a CONTRATANTE fará as retenções devidas ao INSS e as dos impostos e contribuições previstas na **Instrução Normativa SRF nº 1.234, de 11/01/2012.**

Parágrafo terceiro. Caso a CONTRATADA seja optante pelo "SIMPLES" (Lei nº 9.317/96), não serão feitas as retenções de que trata a citada instrução normativa, ficando a CONTRATADA nesse caso obrigada a apresentar declaração, na forma do Anexo IV da mesma Instrução Normativa SRF nº 1.234, de 11/01/2012, em duas vias, assinadas pelo seu representante legal.

Parágrafo quarto. A CONTRATADA deverá, ainda, juntamente à Nota Fiscal / Fatura, apresentar os documentos comprobatórios de regularidade fiscal e trabalhista, exigidos no Edital de Licitação.

Parágrafo quinto. Nenhum pagamento será efetuado à CONTRATADA, enquanto pendente de liquidação qualquer obrigação financeira que lhe for imposta, em virtude de penalidade ou inadimplência contratual, sem que isso gere direito a acréscimos de qualquer natureza.

Parágrafo sexto. Ao CONTRATANTE fica reservado o direito de não efetuar o pagamento se, no momento da aceitação, os serviços prestados, não estiverem em perfeitas condições e em conformidade com as especificações estipuladas.

Parágrafo sétimo. Nos casos de eventuais atrasos de pagamento, desde que a CONTRATADA não tenha concorrido de alguma forma para tanto, fica convencionada a taxa de atualização financeira devida pelo Conselho Nacional do Ministério Público, conforme disposto no art. 36, § 4º, da Instrução Normativa/SLTI-MP n.º 02, de 30/04/2008, mediante a aplicação da seguinte fórmula:

$EM = I \times N \times VP$, sendo

$I = (TX/100)$, assim apurado: $I = (6/100)$ $I = 0{,}00016438$
365 365

Em que:

I = Índice de atualização financeira;

TX = Percentual da taxa de juros de mora anual = 6%;

EM = Encargos moratórios;

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = Valor da parcela em atraso.

Parágrafo oitavo. Aplica-se a mesma regra disposta no parágrafo anterior, na hipótese de eventual pagamento antecipado, observado o disposto no art. 38 do Decreto nº 93.872/86.

CLÁUSULA OITAVA – DA DOTAÇÃO ORÇAMENTÁRIA

As despesas com a execução deste Contrato correrão, neste exercício, à conta de créditos orçamentários consignados no Orçamento Geral da União, Conselho Nacional do Ministério Público, no Programa/Atividade 03.023.2100.8010.0001, na categoria econômica 3.3.9.0.39, subitem 27, para o exercício seguinte, créditos próprios de igual natureza.

Parágrafo único. Para cobertura da despesa foi emitida Nota de Empenho nº 2016NE000409, de 18/08/2016, à conta da dotação orçamentária especificada nesta Cláusula.

CLÁUSULA NONA – DO REAJUSTE DO CONTRATO

O contrato poderá ser reajustado, visando à adequação aos novos preços de mercado e à variação efetiva dos custos de produção, observado o interregno mínimo de 12 (doze) meses, a contar da data de apresentação da proposta ou do orçamento a que essa proposta se referir, ou da data do último reajuste, aplicando-se o *IGP-M/FGV* ou, na insubsistência deste, por outro índice que vier a substituí-lo.

CLÁUSULA DEZ – DAS RESPONSABILIDADES

A CONTRATADA responderá civil e criminalmente pelos prejuízos causados ao patrimônio da União em decorrência de ação ou omissão de seus empregados ou prepostos.

Parágrafo primeiro. A CONTRATADA responderá civilmente pelos furtos e roubos que porventura venham a ocorrer no interior das dependências do CONTRATANTE, nos casos em que ficar

comprovado dolo ou culpa de seus prepostos ou empregados.

Parágrafo segundo. Na hipótese de verificação dos danos, a CONTRATADA ficará obrigada a promover a reposição do bem em condições idênticas ou o ressarcimento a preços atualizados, dentro de 30 (trinta) dias, contados a partir da comprovação de sua responsabilidade.

Parágrafo terceiro. Caso a CONTRATADA não promova a reposição do bem nos termos do Parágrafo segundo desta Cláusula, dentro do prazo estipulado, o CONTRATANTE reserva-se o direito de descontar o valor do ressarcimento da garantia de execução ou da fatura do mês.

CLÁUSULA ONZE – DO RECURSO

É admissível recurso dos atos do CONTRATANTE, decorrentes da execução deste Contrato, no prazo de 05 (cinco) dias úteis a contar da data da respectiva ciência, conforme art. 109, da Lei nº 8.666/93.

CLÁUSULA DOZE – DAS PENALIDADES E RECURSOS

A CONTRATADA ficará sujeita às penalidades previstas nas Leis nº 10.520/2002 e 8.666/93 em caso de descumprimento de quaisquer das cláusulas ou condições do presente Contrato.

Parágrafo primeiro. Conforme o disposto no art. 28 do Decreto nº 5.450, de 31/05/2005 e no Acórdão 754/2015-TCU, a licitante que, dentro do prazo de validade de sua proposta, negar-se a retirar a nota de empenho, deixar de assinar o termo de contrato quando exigido, deixar de entregar a documentação exigida para o certame ou 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 ou cometer fraude fiscal, ficará impedido de licitar e contratar com a União, e, se for o caso, será descredenciado no SICAF, pelo prazo de até 5 anos, sem prejuízo de multa de até 10% (dez por cento) do valor estimado para a contratação e demais cominações legais.

Parágrafo segundo. Caso a contratada não inicie a prestação dos serviços no prazo e demais condições avençadas, estará sujeita à multa de 0,5% sobre o valor total da contratação, por dia de atraso injustificado, limitada sua aplicação até o máximo de 10 dias. Após o 10º dia de atraso, os serviços poderão, a critério do CONTRATANTE, não mais ser aceitos, configurando-se a inexecução total do Contrato, com as consequências previstas em lei e neste instrumento.

Parágrafo terceiro. Uma vez iniciada a execução dos serviços contratados, a sua prestação de forma incompleta ou em desconformidade com as condições avençadas poderá acarretar, além do previsto

nos parágrafos anteriores desta Cláusula, resguardados os procedimentos legais pertinentes:

a) advertência;

b) multa, a ser recolhida no prazo máximo de 5 (cinco) dias úteis, a contar da comunicação oficial, nas hipóteses previstas no item 7 – DAS PENALIDADES do Termo de Referência - Anexo I do Edital.

c) suspensão temporária de participação em licitação e impedimento de contratar com a Administração, por até 02 (dois) anos;

d) declaração de inidoneidade para licitar ou contratar com a Administração Pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a licitante vencedora ressarcir a Administração pelos prejuízos resultantes e após decorrido o prazo da sanção aplicada com base na alínea anterior.

Parágrafo quarto. No caso de não-recolhimento do valor da multa, dentro de 5 (cinco) dias úteis a contar da data da intimação para o pagamento, a importância será descontada da garantia prestada ou dos pagamentos a que fizer jus a CONTRATADA ou ajuizada a dívida, consoante o § 3° do art. 86 e § 1° do art. 87 da Lei n.° 8.666/93, acrescida de juros moratórios de 1,0% (um por cento) ao mês.

Parágrafo quinto. Os atos administrativos de aplicação das sanções previstas nos incisos III e IV, do art. 87, da Lei n.° 8.666/93 e a constantes do art. 7° da Lei n° 10.520/02, bem como a rescisão contratual, serão publicados resumidamente no Diário Oficial da União.

Parágrafo sexto. De acordo com o artigo 88, da Lei n° 8.666/93, serão aplicadas as sanções previstas nos incisos III e IV do artigo 87 da referida lei, à CONTRATADA ou aos profissionais que, em razão dos contratos regidos pela citada lei:

a) tenham sofrido condenação definitiva por praticarem, por meios dolosos, fraudes fiscais no recolhimento de quaisquer tributos;

b) tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;

c) demonstrem não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.

Parágrafo sétimo. Da aplicação das penas definidas no § 1° e no art. 87, da Lei n.° 8.666/93, exceto para aquela definida no inciso IV, caberá recurso no prazo de 05(cinco) dias úteis da data de intimação do ato.

Parágrafo oitavo. No caso de declaração de inidoneidade, prevista no inciso IV, do art. 87, da Lei n.° 8.666/93, caberá pedido de reconsideração ao Exmo. Sr. Presidente do Conselho Nacional do

Ministério Público, no prazo de 10 (dez) dias úteis a contar da data de intimação do ato, podendo a reabilitação ser requerida após 2 (dois) anos de sua aplicação.

Parágrafo nono. Na comunicação da aplicação da penalidade de que trata o item anterior, serão informados o nome e a lotação da autoridade que aplicou a sanção, bem como daquela competente para decidir sobre o recurso.

Parágrafo dez. O recurso e o pedido de reconsideração deverão ser entregues, mediante recibo, no setor de protocolo do CONTRATANTE, localizado no edifício Adail Belmonte, situado no Setor de Administração Federal Sul, Quadra 03 Lote 02, Brasília/DF, nos dias úteis, das 13h às 17h.

Parágrafo onze. As penalidades previstas neste Contrato são independentes entre si, podendo ser aplicadas isoladas ou, no caso de multa, cumulativamente, sem prejuízo de outras medidas cabíveis, garantida prévia defesa (art. 87, § 2º da Lei 8.666/93).

Parágrafo doze. As multas aplicadas são deduzidas do valor do pagamento devido à Contratada, quando possível, ou cobradas por via de procedimento extrajudicial ou judicial, conforme o caso.

CLÁUSULA TREZE – DA RESCISÃO

A inexecução total ou parcial do Contrato poderá ensejar a sua rescisão, conforme disposto nos artigos 77 a 80 da Lei nº 8.666/1993.

Parágrafo primeiro. Os casos de rescisão contratual serão formalmente motivados nos autos do procedimento, assegurado o contraditório e a ampla defesa.

Parágrafo segundo. A rescisão do Contrato poderá ser:

a) Determinada por ato unilateral e escrito do CONTRATANTE nos casos enumerados nos incisos I a XII e XVII do artigo 78 da Lei n.º 8.666/93, mediante notificação através de ofício entregue diretamente ou por via postal, com prova de recebimento, sem prejuízo das penalidades previstas neste Contrato;

b) Amigável, por acordo entre as partes, mediante a assinatura de termo aditivo ao contrato, desde que haja conveniência para o CONTRATANTE; e

c) Judicial, nos termos da legislação.

Parágrafo terceiro. A rescisão unilateral ou amigável deverá ser precedida de autorização escrita e fundamentada da autoridade competente.

Parágrafo quarto. De conformidade com o § 2º do artigo 79, da Lei nº 8.666/93, quando a rescisão ocorrer com base nos incisos XII a XVII do artigo 78 da mesma lei, sem que haja culpa da CONTRATADA, será esta ressarcida dos prejuízos regularmente comprovados que houver sofrido, tendo

ainda direito a:

a) Devolução de garantia, se houver;

b) Pagamentos devidos pela execução do contrato até a data da rescisão;

c) Pagamento do custo de desmobilização.

Parágrafo quinto. A rescisão poderá acarretar as seguintes consequências imediatas:

a) Execução da garantia contratual para ressarcimento, ao CONTRATANTE, dos valores das multas aplicadas ou de quaisquer outras quantias ou indenizações a ela devidas;

b) Retenção dos créditos decorrentes do Contrato, até o limite dos prejuízos causados ao CONTRATANTE.

CLÁUSULA QUATORZE – DA ALTERAÇÃO

Este Contrato poderá, nos termos do art. 65 da Lei nº 8.666/93, ser alterado por meio de Termos Aditivos, objetivando promover os acréscimos ou supressões que se fizerem necessários.

Parágrafo único. Nenhum acréscimo ou supressão poderá exceder o limite estabelecido no parágrafo primeiro do art. 65 da Lei nº 8.666/93, salvo as supressões resultantes de acordos celebrados entre os contratantes.

CLÁUSULA QUINZE – DA VALIDADE

Este Contrato somente terá validade depois de aprovado pelo Sr. Secretário-Geral do Conselho Nacional do Ministério Público.

Parágrafo único. Incumbirá ao CONTRATANTE à sua conta e no prazo estipulado no art. 20 do Decreto n.º 3.555, de 8/8/2000, a publicação do Extrato deste Contrato e dos Termos Aditivos no Diário Oficial da União.

CLÁUSULA DEZESSEIS – DO FORO

Fica eleito o foro da Justiça Federal da cidade de Brasília/DF para dirimir as dúvidas não solucionadas administrativamente, oriundas das obrigações aqui estabelecidas.

E, por estarem de pleno acordo, depois de lido e achado conforme, foi o presente Contrato lavrado em 02 (duas) vias de igual teor e forma, assinado pelas partes e testemunhas abaixo.

Brasília/DF, 13 de setembro de 2016.

CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO
CONTRATANTE

NCT INFORMÁTICA LTDA.
CONTRATADA

TESTEMUNHAS:

NOME:
CPF: 429.800.102-82

Antonio Carlos G. Pinheiro Filho
Diretor de Operações
NCT Informática Ltda.

NOME: Bruno de Sousa Trindade
CPF:

Bruno de Sousa Trindade
Técnico Administrativo
Matrícula: 82.429

APROVO.

Silvio Roberto Oliveira de Amorim Junior
Procurador Regional da República
Secretário-Geral do CNMP

CONSELHO
NACIONAL DO
MINISTÉRIO PÚBLICO

ANEXO I DO CONTRATO Nº 31/2016

TERMO DE REFERÊNCIA

1. DO OBJETO

Contratação de empresa especializada para o fornecimento de serviço de proteção, controle e resposta a incidentes de rede, monitoração dos serviços de filtro de pacote, controle de aplicação, administração de largura de banda, QoS, suporte para conexões VPN IPSec e SSL, IPS, prevenção contra ameaças de vírus, *spywares* e *malwares Zero Day*, filtro de URL, controle de transmissão de dados e acesso à internet com uso de solução, do tipo appliance, com características de *Next Generation Firewall* (NGFW), fazendo parte do serviço o fornecimento, a instalação, configuração de hardware e softwares da solução, para o Conselho Nacional do Ministério Público, conforme especificações constantes neste termo de referência.

2. JUSTIFICATIVA

O Conselho Nacional do Ministério Público – CNMP, cada vez mais tem papel preponderante na realidade de como atua o Ministério Público brasileiro. Na verdade, não teria como ser diferente, uma vez que a própria Constituição Federal registra de maneira clara e direta as atribuições que ensejaram a criação e definem a atuação do órgão.

Como órgão de controle externo da atuação do Ministério Público é de se esperar que meios modernos e eficazes sejam adotados para cumprir de maneira adequada a tarefa, além de contribuírem na prestação de contas à sociedade, observando os princípios mais básicos da transparência pública.

Somando-se a isso, ainda existe a preocupação premente de que a imagem institucional do CNMP seja sempre preservada de fatores externos e nocivos, muitas vezes utilizando-se de iniciativas que visam desenvolver e difundir mentalidade acerca da importância da segurança institucional.

Para que se mantenha imaculada a imagem institucional é necessária que seus integrantes sempre compreendam os requisitos de eficiência e idoneidade adotando medidas cabíveis para incorporem esses conceitos.

Ações diversas são realizadas neste sentido, como o desenvolvimento de sistemas informatizados, preparados com auditoria e controle de segurança, tudo isso impulsionado pela preocupação em se estimular a busca de tecnologias inovadoras que facilitem e otimizem os controles desejados, nos níveis adequados à demanda.

Com o objetivo de aprimorar a atuação constitucional reservada ao Conselho, muitas dessas ações foram planejadas e registradas com o Planejamento Estratégico CNMP para o ciclo 2010-2017 e, como não

podia ser diferente, muitas delas envolvem Tecnologia da Informação – TI.

O objetivo estratégico citado no parágrafo anterior desdobra-se no eixo Sustentação do Ambiente Computacional, principalmente, nas iniciativas Gestão de Contratos Continuados para a Área de Infraestrutura e no eixo – Promoção da Segurança da Informação na iniciativa Ampliação da Segurança de PerímetroSRV08 - Renovação parcial do parque tecnológico, constante do PDTI do CNMP para o ano 2015. As ações concentram os investimentos em ativos destinados a aumentar a robustez do ambiente operacional do Conselho, elevando os níveis de performance, segurança e de tolerâncias a falhas a fim de garantir a qualidade e níveis dos serviços providos.

Neste mesmo contexto, cabe ainda o registro que, foi implantado o Sistema de Processo Eletrônico do CNMP, batizado de sistema ELO, o qual foi concebido e programado para possibilitar maior celeridade na tramitação processual, conferindo ao órgão maior capacidade em atender o público pretendido. Esse sistema, é responsável pela mudança da forma como os autos processuais são produzidos e trabalhados, passando a ser totalmente digitais e eletrônicos.

A fim de complementar esse novo sistema, entrará no ar também nova sistemática de publicação dos atos do CNMP por intermédio do Diário Eletrônico que terá a função de substituir, em grande parte, a sistemática adotada atualmente que envolve publicações oficiais menos acessíveis.

Em contrapartida, com base nos objetivos e ações de melhoria da atuação do CNMP impostos, faz-se necessário que o Conselho também tenha meios para obter informações sensíveis para que seja possível a realização de auditorias e outras contramedidas em casos de riscos que tenham se concretizado, a fim de que a segurança institucional possa ser mantida junto com a própria imagem institucional.

Logo, para que esses dois sistemas funcionem plenamente, outras ações de TI complementares foram planejadas e formalizadas visando especificamente subsidiar as questões relativas à segurança institucional por meio da adoção ou melhoria dos mecanismos de respostas a incidentes que venham ocorrem nesses novos serviços.

Nesta linha, as iniciativas de Gestão de Contratos Continuados para a Área de Infraestrutura e Ampliação da Segurança de Perímetro são iniciativas de TI que, em sua essência, foram planejadas para tratar os aspectos estruturantes das outras ações, e contribuem para concretizar as medidas necessárias para salvaguarda das questões relativas à segurança e imagem institucional.

Então, para atender a atender a nova realidade do CNMP, a qual demanda publicação de serviços visando a maior disponibilidade possível, a STI realizou processo de compra de dois novos canais de comunicação de dados, que funcionarão em contingência ativa, com características adequadas para tal finalidade como forma de substituir os atuais. Estes canais, por sua vez, não possuem qualquer serviço de segurança ou controle de banda, o que torna necessária a contratação da solução objeto deste termo.

A contratação da solução de segurança sob a forma de serviço continuado visa atender aos princípios de eficiência e economicidade, visto que a simples aquisição do equipamento que sustenta a solução não seria suficiente para atender às necessidades do CNMP, que incluem, por exemplo, o monitoramento de acessos e tentativas de ataque, 24 horas do dia, 7 dias por semana. Além disso, seriam necessários investimentos em instalação, configuração, manutenção, suporte, atualização, preservação da disponibilidade e treinamento de técnicos do CNMP para a administração da solução. Pesa ainda a questão de obsolescência inerente a equipamentos de informática, tanto com relação à capacidade do dispositivo em atender a uma determinada demanda e seu crescimento, quanto à qualidade e à eficiência técnica. A constante evolução das ameaças e a correspondente necessidade de resposta dos algoritmos de detecção e prevenção de intrusão e códigos maliciosos formam desafios difíceis de serem continuamente superados. Contratados sob a forma de serviço, os equipamentos obsoletos ou tecnicamente defasados envolvidos na solução podem ser substituídos quando não mais atenderem ao acordo de nível de serviço (SLA) ou deixarem de ser viáveis tecnicamente e/ou economicamente

O prazo de vigência contratual de **60** meses é necessário para permitir não só a empresa a amortização do seu investimento nos equipamentos que serão adquiridos para prestação do serviço, possibilitando diminuir o valor cobrado devido a segurança de retorno do investimento, propiciando ao CNMP a economia na contratação do serviço, bem como se torna mais eficiente do ponto de vista da continuidade do serviço uma vez que, a cada troca de fornecedor do serviço, uma série de atividades prévias e posteriores ao vencimento do contrato precisam ser desenvolvidas, como migração do ambiente para nova solução, reabsorção do conhecimento da infraestrutura do CNMP pela nova empresa, recapacitação dos servidores do órgão caso haja troca de tecnologia, dentre outras. Atividades que oneram e impactam diretamente em um serviço de tal criticidade.

3. DESCRIÇÃO DOS SERVIÇOS

3.1. A CONTRATADA deverá monitorar, operar e administrar os serviços da solução de forma remota, em regime de 24 (vinte e quatro) horas por dia, 7 (sete) dias da semana, 365 (trezentos e sessenta e cinco) dias por ano.

3.2. A CONTRATADA deverá manter atualizados os equipamentos destinados à execução dos serviços, implementando as últimas versões estáveis (se for o caso), atualizações e correções de hardware e software recomendadas pelo fabricante, de modo a assegurar a plena integridade, segurança e o desempenho do ambiente em produção, de forma programada em acordo com a equipe de infraestrutura de produção do CNMP.

3.3. A CONTRATADA deverá, por meio da administração remota, ser capaz de implementar políticas, regras, filtros ou quaisquer outros recursos e implementações lógicas, necessárias a manutenção do serviço em conformidade com o especificado. As solicitações de alterações e inclusões de novos políticas, regras e filtros efetuados pelo contratante não serão limitadas e deverão ser implementadas, de acordo com o SLA. As solicitações poderão ser feitas e acompanhadas pelo contratante via portal web seguro, por número telefônico gratuito e e-mail.

3.4. A CONTRATADA deverá criar contas de acesso privilegiado à administração dos serviços para a equipe técnica do CONTRATANTE, que permitam a execução de funções de administração da solução, em especial alterações e inclusões de novas políticas, regras e filtros. Todos os acessos à administração dos serviços, inclusive aqueles efetuados pela contratada, deverão ser autenticados, criptografados e registrados para posterior auditoria.

3.5. Caberá à CONTRATADA o registro, monitoração, triagem e classificação prévia de severidade de todos os alertas de incidentes emitidos pelos serviços administrados, em especial os relacionados a tentativas de ataques em direção à rede do CONTRATANTE ou por ela originados; e adotar, de imediato, as medidas de tratamento automático que forem acordadas com o CONTRATANTE, cabendo a este a classificação final da severidade. Tais medidas estarão relacionadas com o grau de severidade constante na assinatura do ataque indicado pelo Serviço de Prevenção de Intrusão. Para incidentes de maior grau de severidade, a CONTRATADA deverá notificar a equipe técnica do CONTRATANTE por ligação telefônica, correio eletrônico e mensagens SMS (Short Message Service).

3.6. Caso seja necessária a instalação de equipamentos de administração da solução nas instalações do CONTRATANTE, a CONTRATADA deverá fornecer todos os recursos necessários para tanto, incluindo a disponibilização de rack adequado à instalação dos equipamentos. O CONTRATANTE ficará responsável apenas pelo fornecimento de alimentação elétrica e portas lógicas para as conexões.

3.7. O acesso aos equipamentos de administração eventualmente hospedados no CNMP dar-se-á por meio de VPNs via Internet, a serem implementadas pela CONTRATADA. De forma a possibilitar a administração remota, a CONTRATADA poderá optar por proceder a instalação e a manutenção de canal de comunicação direto com os equipamentos sob sua responsabilidade, devendo se responsabilizar e garantir total segurança para este acesso. Atuações locais, que necessitem de acesso físico direto ao ambiente e ao equipamento, deverão ser previamente comunicados e acordados com a equipe do CNMP.

3.8. Todos os equipamentos responsáveis pela execução dos serviços contratados deverão ser acessíveis a partir de plataformas de gerenciamento SNMP localizadas na rede interna do CONTRATANTE.

3.9. Os equipamentos que compõem a solução deverão ter seu funcionamento restrito às suas funções, não podendo interferir ou causar lentidão no funcionamento das redes locais das unidades do CONTRATANTE.

3.10. Após a assinatura do contrato, o contratante informará à contratada os endereços IP dos seus sistemas de gerenciamento de rede (NMS) que deverão estar autorizados a realizar consultas SNMP (get) nos equipamentos da rede e o nome da comunidade (community string) que deverá ser configurado.

3.11. A instalação, remoção ou desabilitação das funcionalidades dos equipamentos deverá, sempre que possível, ser realizada sem que outros componentes da rede local do CONTRATANTE necessitem de configuração adicional.

3.12. A CONTRATADA deverá desempenhar suas atividades por intermédio de técnicos devidamente especializados e qualificados nos equipamentos que darão suporte aos serviços e caso seja constatada a falta de conhecimento mínimo necessário para operação da solução por parte do prestador de serviço, a equipe técnica do Conselho poderá solicitar sua substituição por técnico devidamente qualificado.

3.13. A empresa proponente deverá fazer constar em sua proposta a marca e o modelo dos equipamentos que darão suporte aos serviços descritos.

4. DAS ESPECIFICAÇÕES TÉCNICAS MÍNIMAS

CARACTERÍSTICAS GERAIS

Os serviços deverão ser prestados por um **conjunto de equipamentos em *cluster (exceto para aqueles itens onde especifica-se o contrário)***,, do tipo *appliance*, não sendo admitidas alternativas baseadas em computadores de uso geral/comum. Esses equipamentos deverão ser fornecidos pela CONTRATADA e instalados na rede da Sede do CNMP. Os equipamentos deverão suportar a implantação de zona desmilitarizada (DMZ), além de segmentos de distintos de rede, como externa e interna. Todos os equipamentos que comporão a solução no cluster deverão operar em regime de alta disponibilidade por meio de dois equipamentos idênticos, de forma que a falha em um deles não implique em interrupção dos serviços contratados e nem em perda de desempenho da solução.

A CONTRATADA deverá realizar todo repasse de conhecimento relativo à instalação, gerenciamento, operacionalização, manuseio, configuração da solução, visando a possibilidade de atuação por parte da equipe técnica do CNMP quando necessário, em formato a ser definido pela CONTRATANTE.

4.1. A fim de atender as necessidades/demanda geradas pelos usuários e infraestrutura tecnológica do Conselho, a solução deverá ser implementada através de plataforma de segurança de tenha, no mínimo, a capacidade e as características abaixo:

a) *Throughput* de 2 Gbps, baseado em conexões TCP/IP, com a funcionalidade de controle de aplicação habilitada para todas as assinaturas que o fabricante possuir;
b) *Throughput* de 1 Gbps, baseado em conexões TCP/IP, com as funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes, como controle de aplicação IPS, Antivírus e *Antispyware*;
c) Suporte a, no mínimo, 240.000 conexões simultâneas;
d) Suporte a, no mínimo, 45.000 novas conexões por segundo;
e) Fonte 120/240 AC;
f) Possuir Interfaces de rede 10/100/1000 base-TX suficientes para atender a no mínimo 5 segmentos de rede;
g) Possuir Interfaces de rede 1 Gbps SFP suficientes para atender a no mínimo 5 segmentos de rede;
h) Interfaces dedicadas suficientes para funcionar cluster de alta disponibilidade;
i) 1 (uma) interface de rede 1 Gbps dedicada para gerenciamento;
j) 1 (uma) interface do tipo console ou similar;
k) Suporte a, no mínimo, 30 (trinta) segmentos de rede distintos;
l) Suportar 100 (cem) clientes de VPN SSL simultâneos;
m) Suportar 100 (cem) túneis de VPN IPSEC simultâneos;
n) Estar licenciado ou suportar nativamente no mínimo, 5 (cinco) sistemas virtuais lógicos (Contextos) no firewall físico, sendo que os contextos virtuais devem suportar as funcionalidades nativas da plataforma de segurança incluindo: Firewall, IPS, Antivírus, *Antispyware*, Filtro de URL, Filtro de Dados VPN, Controle de Aplicações, QOS, NAT e Identificação de usuários;
o) A console de gerência e monitoração devem, preferencialmente, residir no mesmo *appliance* de proteção de rede, e possuir recursos de CPU, memória, interface de rede e sistema operacional dedicados para esta função, afim de garantir a disponibilidade de gerenciamento mesmo quando o equipamento esteja sobre ataque ou enfrentando alguma intermitência.

1. No caso da necessidade de utilização de hardware e/ou software suplementar para esta funcionalidade, estes deverão, necessariamente, obedecer às mesmas premissas acima elencadas e ser fornecidos e administrados/operados pela Contratada, a qual também se responsabilizará por qualquer ocorrência e/ou risco gerado no ambiente tecnológico do Conselho em função destes dispositivos e devem possuir.

p) Na data da entrega, nenhum dos modelos ofertados e componentes da solução, poderão estar listados pelo fabricante em listas de equipamentos descontinuados ou fora de linha;

q) A solução deve ter total integração com Microsoft Active Directory, LDAP e Novell eDirectory, preferencialmente sem a necessidade de instalação ou utilização de nenhum software adicional, como agente, servidor ou cliente, para todas as funcionalidades desta especificação que permitam ou exijam identificação e/ou autenticação de usuário, como: criação de políticas por usuário para controle de aplicação, IPS, antivirus, anti-spyware, filtro de arquivos, filtro de URL, QOS (Traffic Shaping e marcação de pacotes), autenticação via Captive Portal, extração de relatórios por usuários, dentre outras funcionalidades. No caso da necessidade de instalação e/ou utilização de hardware e/ou software adicional em servidor ou cliente, estes deverão, necessariamente, serem fornecidos e administrados/operados pela Contratada, a qual também se responsabilizará por qualquer ocorrência e/ou risco gerado no ambiente tecnológico do Conselho em função destes dispositivos.

r) Deve permitir a total customização das páginas de erro, categorização, captive portal, dentre outras necessárias a integração com a identidade funcional do órgão;

4.2. A solução deve consistir de appliances de proteção de rede com funcionalidades de Next Generation Firewall (NGFW);

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

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

4.5. Todos os equipamentos fornecidos devem acompanhar rack 19", que deve ser fornecido pela contratada, incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;

4.6. Os softwares utilizados deverão ser fornecidos em sua versão estável mais atualizada;

4.7. A solução deve possuir pelo menos as seguintes funcionalidades:

a) Suporte a pelo menos 4094 VLAN Tags 802.1q;

b) Agregação de links 802.3ad;

c) Policy based routing ou policy based forwarding;

d) Roteamento multicast (PIM-SM);

e) DHCP Relay;

f) DHCP Server;

g) Jumbo Frames;

h) Suporte à criação de objetos de rede que possam ser utilizados como endereço IP de interfaces L3;

4.8. A solução deve suportar sub-interfaces ethernet lógicas;

4.9. A solução deve suportar os seguintes tipos de NAT:

a) Nat dinâmico (Many-to-1);

b) Nat dinâmico (Many-to-Many);

c) Nat estático (1-to-1);

d) NAT estático (Many-to-Many);

e) Nat estático bidirecional 1-to-1;

f) Tradução de porta (PAT);

g) NAT de Origem;

h) NAT de Destino;

i) Suportar NAT de Origem e NAT de Destino simultaneamente;

4.10. A solução deve ser capaz de enviar registros de log para serviços de monitoração externos, simultaneamente, via protocolo TCP/IP e SSL;

a) Deve permitir configurar certificado caso necessário para autenticação no sistema de monitoração externo de logs;

4.11. A solução deve possuir proteção anti-spoofing;

4.12. A solução deve suportar roteamento estático e dinâmico para IPv4 (RIPv2, BGP e OSPFv2) e IPv6 (OSPFv3);

4.13. A solução deve suportar OSPF graceful restart;

4.14. A solução deve suportar IPv6. No caso da necessidade de instalação e/ou utilização de hardware e/ou software adicional em servidor ou cliente, estes deverão, necessariamente, serem fornecidos e administrados/operados pela Contratada, a qual também se responsabilizará por qualquer ocorrência e/ou risco gerado no ambiente tecnológico do Conselho em função destes dispositivos.

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

a) Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;

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

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

d) Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;

4.16. A solução deve ter suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo, em modo transparente e layer 3;

4.17. A configuração em alta disponibilidade deve sincronizar:

a) Sessões;

b) Configurações, incluindo, mas não limitado a políticas de Firewall, NAT, QOS e objetos de rede;

c) Certificados de-criptografados;

d) Associações de Segurança das VPNs;

e) Tabelas FIB;

4.18. O modo de alta disponibilidade deve possibilitar monitoração de falha de link, e ser capaz de transferir todo o tráfego para o link operacional de modo transparente e automático;

CONTROLE DE POLÍTICAS DE FIREWALL

A solução deverá suportar, no mínimo:

4.19. Controles de segurança por segmento distinto.

4.20. Controles de políticas por porta e protocolo.

4.21. Controle de políticas por aplicações, grupos estáticos ou dinâmicos de aplicações (baseados não apenas em assinaturas, mas em características e comportamento das aplicações - Heurística) e categorias de aplicações.

4.22. Controle de políticas por usuários, grupos de usuários, IPs, redes e segmentos de rede.

4.23. Controle de políticas por código de País (Por exemplo: BR, USA, UK, RUS).

4.24. Controle, inspeção e decriptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound).

4.25. Offload de certificado em inspeção de conexões SSL de entrada (Inbound);

4.26. Descriptografia de tráfego Inbound e Outbound em conexões negociadas com TLS 1.2;

4.27. Controle de inspeção e de-criptografia de SSH por política;

4.28. A plataforma de segurança deve permitir a descriptografia de tráfego (SSL e TLS), sendo permitido para esta funcionalidade o uso de appliance externo específico.

4.29. Controle de download ou envio de arquivos, por tipo, extensão e mime-type (assinatura), como: bat, cab, dll, exe, pif, e reg, zip, mp3, mp4, dentre outros.

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

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

4.32. Objetos e regras IPV6.

4.33. Objetos e regras multicast.

4.34. A atribuição de agendamento com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.

CONTROLE DE APLICAÇÕES

Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo com, no mínimo, as seguintes funcionalidades:

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

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

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

4.38. Deve inspecionar o payload de pacote de dados com o objetivo de detectar através de expressões regulares assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo. A checagem de assinaturas também deve determinar se uma aplicação está utilizando a porta default ou não, como por exemplo a utilização de RDP na porta 80 ao invés da sua porta padrão;

4.39. Deve aplicar heurística a fim de detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a Encrypted Bittorrent, ULTRASURF e aplicações VOIP que utilizam criptografia proprietária;

4.40. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e ataques mediante a porta 443.

4.41. Para tráfego criptografado (SSL e SSH), deve descriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;

4.42. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado, a Yahoo Instant Messenger usando HTTP. A decodificação de protocolo também deve identificar funcionalidades especificas dentro de uma aplicação, incluindo, mas não limitado, a compartilhamento de arquivo dentro do Webex. Além de detectar arquivos e outros conteúdos que devem ser inspecionados de acordo as regras de segurança implementadas;

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

4.44. Atualizar a base de assinaturas de aplicações automaticamente;

4.45. Reconhecer aplicações em IPv6;

4.46. Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e/ou grupos do LDAP, Microsoft Active Directory, Novell eDirectory e base de dados local;

4.47. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, LDAP, Novell eDirectory e base de dados local. No caso da necessidade de instalação e/ou utilização de hardware e/ou software adicional em servidor ou cliente, estes deverão, necessariamente, serem fornecidos e administrados/operados pela Contratada, a qual também se responsabilizará por qualquer ocorrência e/ou risco gerado no ambiente tecnológico do Conselho em função destes dispositivos.

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

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

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

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

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

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

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

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

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

4.57. Deve possibilitar a diferenciação e controle de partes das aplicações, como por exemplo, permitir o Gtalk chat e bloquear a transferência de arquivos;

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

4.59. Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como:

a) Tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc).

b) Nível de risco da aplicação.

c) Categorização de aplicações.

d) Aplicações que usem técnicas evasivas, utilizadas por malwares, como transferência de arquivos e/ou uso excessivo de banda, etc.

PREVENÇÃO DE AMEAÇAS

4.60. Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de Firewall ou serem entregues através de composição com outro equipamento ou fabricante, respeitando as características mínimas necessárias especificadas neste TR, como o funcionamento em alta disponibilidade através de cluster de equipamentos idênticos.

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

4.62. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;

4.63. Quando utilizada as funções de IPS, Antivírus e Anti-spyware, o equipamento deve manter performance compatível com os níveis de desempenho previsto no Edital (item 6.2) sem que haja degradação do serviço prestado, independentemente do quantitativo de assinaturas habilitadas de IPS, Anti-Vírus e Antispyware simultaneamente.

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

4.65. Exceções por IP de origem ou de destino devem ser possíveis nas regras, de forma geral e assinatura a assinatura;

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

4.67. Deve permitir o bloqueio de vulnerabilidades.

4.68. Deve permitir o bloqueio de exploits conhecidos.

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

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

a) Análise de padrões de estado de conexões;

b) Análise de decodificação de protocolo;

c) Análise para detecção de anomalias de protocolo;

d) Análise heurística;

e) IP Defragmentation;

f) Remontagem de pacotes de TCP;

g) Bloqueio de pacotes malformados.

4.71. Ser imune e capaz de impedir ataques básicos como: Synflood, ICMPflood, UDPfloof, etc;

4.72. Detectar e bloquear a origem de portscans;

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

4.74. Suportar os seguintes mecanismos de inspeção contra ameaças de rede: análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, análise heurística, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados;

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

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

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

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

4.79. Suportar bloqueio de arquivos por tipo;

4.80. Identificar e bloquear comunicação com botnets;

4.81. Deve suportar várias técnicas de prevenção, incluindo Drop e tcp-rst (Cliente, Servidor e ambos);

4.82. Deve suportar referência cruzada com CVE;

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

4.84. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS;

4.85. Deve permitir que na captura de pacotes por assinaturas de IPS seja definido o número de pacotes a serem capturados. Esta captura deve permitir selecionar, no mínimo, 50 pacotes;

4.86. Deve possuir a função resolução de endereços via DNS, para que conexões com destino a domínios maliciosos sejam resolvidas pelo Firewall com endereços (IPv4 e IPv6), previamente definidos;

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

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

4.89. Deve incluir proteção contra downloads involuntários usando HTTP de arquivos executáveis. maliciosos.

4.90. Deve possuir rastreamento de vírus em pdf.

4.91. Deve permitir a inspeção em arquivos comprimidos que utilizam o algoritmo deflate (zip, gzip, etc.)

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

FILTRO DE URL

A plataforma de segurança deve possuir, no mínimo, as seguintes funcionalidades de filtro de URL:

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

4.94. Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs, Redes e Zonas de segurança.

4.95. Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via LDAP, Active Directory, Novell eDirectory e base de dados local.

4.96. Permitir popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório;

4.97. Suportar a criação de políticas baseadas no controle por URL e Categoria de URL;

4.98. Deve possuir opção de habilitar a função de Safe Search no acesso a sites de busca (Google, Bing e Yahoo), caso a opção esteja desabilitada. Deve ainda exibir página de bloqueio fornecendo instruções ao usuário de como habilitar a função;

4.99. Suportar base ou cache de URLs local no appliance, evitando delay de comunicação/validação das URLs;

4.100. Possuir categorias de URLs;

4.101. Suportar a criação categorias de URLs customizadas;

4.102. Suportar a exclusão de URLs do bloqueio, por categoria;

4.103. Permitir a customização de página de bloqueio;

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

4.105. Suportar a inclusão nos logs do produto de informações das atividades dos usuários;

IDENTIFICAÇÃO DE USUÁRIOS

4.106. Deve permitir a criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações, através da integração/autenticação, preferencialmente nativa, via LDAP, Active Directory, Novell eDirectory e base de dados local. No caso da necessidade de instalação ou utilização de software adicional em servidor ou cliente, os dispositivos (de hardware e software) adicionais deverão, necessariamente, serem fornecidos e administrados/operados pela Contratada.

4.107. A solução deve suportar o recebimento de eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via syslog, para a identificação de endereços IP e usuários. Cabe o registro de que, caso o equipamento principal provedor da solução não suporte esta característica, fica facultado a contratada, a utilização de outros dispositivos (fornecidos por ela) para realizar a integração;

4.108. Deve permitir o controle, preferencialmente, sem a necessidade de instalação ou utilização de software adicional em servidor ou cliente, em equipamentos que solicitem saída a internet, para que antes de iniciar a navegação, expanda-se um portal para autenticação, através de LDAP, Active Directory, Novell eDirectory e base de dados local, residente no firewall (Captive Portal). No caso da necessidade de instalação e/ou utilização de hardware e/ou software adicional em servidor ou cliente, estes deverão, necessariamente, serem fornecidos e administrados/operados pela Contratada, a qual também se responsabilizará por qualquer ocorrência e/ou risco gerado no ambiente tecnológico do Conselho em função destes dispositivos.

4.109. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server.

4.110. Deve permitir visibilidade e controle granular por usuário sobre o uso das aplicações que estão em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server.

4.111. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em servidores acessados remotamente, mesmo que não sejam servidores Windows.

CONFORMAÇÃO DE TRÁFEGO

Com a finalidade de controlar aplicações, como Youtube, Ustream, Vimeo, dentre outros e tráfegos cuja utilização possa gerar um alto consumo de largura de banda, requer que a solução além de poder permitir ou negar esses tipos de aplicações, deve ter a capacidade de controlá-las por políticas de máxima utilização de largura de banda.

A plataforma de segurança deve:

4.112. Suportar a criação de políticas de QoS por:

a) Endereço de origem

b) Endereço de destino

c) Por usuário e grupo do LDAP, Microsoft Active Directory, Novell eDirectory e Base Local

d) Por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;

e) Por porta;

4.113. O QoS deve possibilitar a definição de classes por:

a) Banda Garantida

b) Banda Máxima

c) Fila de Prioridade.

4.114. Suportar priorização Real Time de protocolos de voz (VOIP) como, mas não se limitando a H.323, SIP e aplicações como Skype.

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

4.116. Disponibilizar estatísticas RealTime para classes ou perfis de QoS.

4.117. Deverá permitir o monitoramento do uso que as aplicações fazem por volume (bytes), sessões e por usuário.

FILTRO DE DADOS

A plataforma de segurança deve:

4.118. Permitir a criação de filtros para arquivos e dados pré-definidos, sendo que estes devem ser identificados por extensão e assinaturas;

4.119. Permitir identificar e prevenir a transferência de vários tipos de arquivos (como DOC, PDF, etc.) sobre aplicações;

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

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

4.122. Permitir listar o número de aplicações suportadas para controle de dados;

4.123. Permitir listar o número de tipos de arquivos suportados para controle de dados;

GEOLOCALIZAÇÃO

A plataforma de segurança deve:

4.124. Suportar a criação de políticas por geolocalização, permitindo que o tráfego de determinados Países seja bloqueado.

4.125. Possibilitar a visualização dos países de origem e destino nos logs dos acessos.

4.126. Possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas.

VPN

A plataforma de segurança deve:

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

4.128. Suportar IPSec VPN;

4.129. Suportar SSL VPN;

4.130. A VPN IPSEc deve suportar:

a) 3DES;

b) Autenticação MD5 e SHA-1;

c) Diffie-Hellman Group 1 , Group 2, Group 5 e Group 14;

d) Algoritmo Internet Key Exchange (IKE);

e) AES 128, 192 e 256 (Advanced Encryption Standard)

f) Autenticação via certificado IKE PKI.

4.131. A VPN SSL deve:

a) Permitir que o usuário realize a conexão de VPN SSL através de Browser, sem a necessidade de instalação de cliente.

b) Permitir autenticação através de Microsoft Active Directory, LDAP, Novell eDirectory , Base de dados Local, Secure ID e Certificado Digital, sem a necessidade de instalação ou utilização de nenhum software agente, servidor ou cliente, adicional;

c) Ser compatível e manter compatibilidade com, pelo menos, os browsers Internet Explorer, Google Chrome, Mozila Firefox em suas últimas versões;

d) Possuir cliente web, disponível diretamente no portal após login, que permita a administração de servidores Linux e Windows através de conexões SSH , RDP e VNC sem a necessidade de instalação de cliente na estação do usuário;

e) Permitir autenticação de 2 fatores.

4.132. Deve possuir interoperabilidade com outros fabricantes, como: Cisco, Checkpoint, Juniper, Palo Alto Networks, Fortinet, Sonic Wall, dentre outros.

4.133. Prover atribuição de endereço IP nos clientes remotos de VPN;

4.134. Prover atribuição de DNS nos clientes remotos de VPN;

4.135. Prover VPN com geração de senha e autosserviço de troca através de portal próprio personalizável;

4.136. Permitir criar políticas de controle de aplicações, IPS, Antivirus, Anti-spyware e filtro de URL para tráfego dos clientes remotos conectados na VPN;

4.137. Suportar proxy arp e uso de interfaces PPPOE;

4.138. Permitir estabelecer um túnel VPN client-to-site do cliente a plataforma de segurança, fornecendo uma solução de single-sign-on aos usuários, integrando-se com as ferramentas de Windows Logon;

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

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

4.141. O agente de VPN a ser instalado nos equipamentos desktop e laptops, deve ser capaz de ser distribuído de maneira automática através de recursos como Microsoft SMS, Active Directory, e/ou por meio da geração de pacotes de instalação MSI e ser descarregado diretamente desde o seu próprio portal, o qual residirá no centralizador de VPN;

4.142. O agente deverá comunicar-se com o portal para determinar as políticas de segurança do usuário;

4.143. Permitir que a conexão com a VPN seja estabelecida das seguintes formas:

a) Antes do usuário autenticar na estação;

b) Sob demanda do usuário;

4.144. Manter uma conexão segura com o portal durante a sessão.

4.145. O agente de VPN client-to-site deve ser compatível com pelo menos: Windows XP, Windows 7, Windows 8, Principais distribuições Linux e Mac OS;

4.146. Deverá possuir compatibilidade com cliente nativo de VPN client-to-site IPsec de, pelo menos: Linux, IOS e Android;

4.147. Estar licenciada para suportar 250 (duzentos e cinquenta) clientes de VPN SSL simultâneos;

4.148. Estar licenciada para suportar 250 (duzentos e cinquenta) túneis de VPN IPSEC simultâneos;

4.149. É permitido o uso de appliance externo para controle de VPN.

MAIL RELAY, ANTISPAM e ANTIMALWARE DE EMAIL

Funcionar como gateways principais de e-mail do domínio cnmp.mp.br e seus subdomínios tanto para envio como para o recebimento de mensagens respeitando todas as normas vigentes no que tange os aspectos de encaminhamento de mensagens, blacklist,graylist, whitelist, autenticação, etc.

Deve-se levar em consideração os seguintes parâmetros para dimensionamento da solução:

- 800 caixas de e-mail
- Tráfego médio de 50 mil mensagens por hora
- Possibilidade de utilização de 5 domínios distintos

A solução deve ser capaz de, no mínimo:

4.150. Reter por, no mínimo, 30 dias todas as mensagens dos usuários classificadas como indevidas, com possibilidade de liberação, exclusão definitiva, adicionar em black ou White list por parte do usuário.

4.151. Permitir controle de quarentena por usuário através de login e senha autenticados em Novell Edirectory, Windows Active Directory e LDAP

4.152. Armazenar por no mínimo 60 dias todos os logs de envio e recebimento de email com no mínimo as seguintes informações: remetente, destinatário, data e hora, assunto, estado da mensagem (entregue, descartada, quarentena, dentre outras)

4.153. Processar todo o tráfego em sua capacidade máxima com todas as funcionalidades de Antispam, Antivirus, Anti-Spyware, Anti-Phishing ativadas.

A solução deve possuir, no mínimo, as seguintes características/funcionalidades:

4.154. Possuir função de Antispam, Antivírus, Anti-Spyware e Anti-Phishing.

4.155. Realizar inspeção do tráfego de entrada e saída de email

4.156. Conectar-se em tempo real em uma base de dados centralizada do fabricante para baixar atualizações de anti-spam

4.157. Possuir proteção contra-ataques de negação de serviço do tipo Mail Bomb

4.158. Possuir controles de DNS Reverso para garantir proteção Anti-Spoofing.

4.159. Possuir controle de limite da taxa de e-mails enviados, por usuário e por grupo de usuários

4.160. Suportar múltiplos domínios de e-mail

4.161. Suportar aplicação de políticas de e-mail por destinatário, por domínio, por tráfego de entrada ou de saída.

4.162. Permitir a criação de perfis de configuração granulares, onde cada perfil agrega definições específicas de funcionalidades como Anti-Spam, Anti-Vírus, Autenticação, entre outras.

4.163. Operar como gateway de correio SMTP para servidores de correio existentes. Realizar quarentena de e-mail com possibilidade de acesso, por usuário, via console web de gerência.

4.164. Enviar relatórios de quarentena aos usuários de e-mail, de forma agendada.

4.165. Realizar arquivamento (archiving) baseado em políticas de mensagens recebidas e enviadas, com suporte à armazenamento remoto

4.166. Suportar gerenciamento de fila de e-mail para mensagens falhas, atrasadas e não entregues

4.167. Realizar autenticação SMTP via LDAP, RADIUS, POP3 ou IMAP

4.168. Manter uma lista de reputação de remetentes locais com base em: número de vírus enviados, a quantidade de spam, número errado de destinatários

4.169. Filtrar anexos e conteúdo das mensagens de e-mail.

4.170. Realizar inspeção de cabeçalhos de e-mail.

4.171. Realizar filtragem estatística Bayesiana.

4.172. Utilizar listas de bloqueio em tempo real usando URIs e / ou URLs de Spam

4.173. Realizar filtragem por palavra proibida (Banned Word)

4.174. Permitir a administração de SPAM com capacidade de Aceitar, Reenviar (Relay), Rejeitar (Reject) ou descartar (Discard)

4.175. Realizar análise de imagem e escaneamento de PDF para detectar spam

4.176. Suportar Black List de terceiros

4.177. Deve suportar endereçamento IPv4 e IPv6

4.178. Suportar Greylisting para IPV4, IPV6 e contas de e-mail

4.179. Suportar detecção de IPs falsificados (Forged IP)

4.180. Suportar White/Black List (usuários / IPs permitidos ou negados) em nível global por equipamento e personalizado por usuário

4.181. Suportar o escaneamento de antivírus / antispyware de arquivos compactados: ZIP, PKZIP, LHA, ARJ, RAR

4.182. Permitir a personalização de mensagens de notificação de Antivirus / AntiSpyware

4.183. Realizar bloqueio por tipo de arquivo

4.184. Suportar modo de operação Gateway, atuando como MTA (Mail Transfer Agent) ou Gateway de E-mail, encaminhando e-mail de/para servidores de e-mail protegidos.

4.185. Suportar modo de operação Transparente, realizando proxy ou encaminhamento (relay) transparente de/para os servidores de e-mail protegidos.

4.186. Suportar modo de operação Servidor, operando como um servidor independente de e-mail e MTA. Deve armazenar e-mails localmente para entrega aos usuários via Webmail, POP3 e IMAP.

4.187. Possuir armazenamento local ou remoto de e-mails.

4.188. Possuir interface de configuração via Web (HTTP, HTTPS)

4.189. Suportar a configuração de administradores do sistema por domínio, sendo possível restringir o acesso por endereço ip e máscara de rede de origem.

4.190. Suportar no mínimo dois níveis de administração: Read / Write (Leitura / Gravação) e Read Only (Somente leitura).

4.191. Suportar a geração e armazenamento de mensagens de log locais e servidores remotos Syslog.

4.192. Gerar relatórios de atividade analisando os arquivos de log, apresentando-os em formato tabular e gráfico.

4.193. Suportar a geração de relatórios sob demanda ou agendados em intervalor específico e formato PDF ou HTML

4.194. Em modo de Alta Disponibilidade, deve suportar monitoramento de estado de enlace, modo de operação ativo-passivo, detecção e notificação de falhas do dispositivo, sincronização de quarentena e fila de e-mail. Não devendo haver perda de e-mails ou alterações de configuração em caso de failover.

4.195. Suportar detecção de Newsletter.

CONSOLE DE GERÊNCIA E MONITORAÇÃO

Quanto ao console de gerência e monitoração, a plataforma de segurança deve:

4.196. Centralizar a administração de regras e políticas do cluster, usando uma única interface de gerenciamento;

4.197. Suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;

4.198. Todo o gerenciamento da solução deve poder ser feito através de console e interface web compatível com os browsers Firefox, Chrome e Internet Explorer;

4.199. O gerenciamento deve permitir/possuir no mínimo, mas não se limitando a:

a) Criação e administração de políticas de firewall e controle de aplicação;

b) Criação e administração de políticas de IPS, Antivírus e Anti-Spyware;

c) Criação e administração de políticas de Filtro de URL;

d) Monitoração de logs;

e) Ferramentas de investigação de logs;

f) Debugging;

g) Captura de pacotes.

4.200. Permitir acesso concorrente de administradores;

4.201. Possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

4.202. Permitir usar palavras chaves e cores para facilitar identificação de regras;

4.203. Permitir monitorar via SNMP falhas de hardware, inserção ou remoção de fontes, discos e coolers (quando for o caso), uso de recursos por número elevado de sessões, número de túneis estabelecidos na VPN cliente-to-site e número de sessões estabelecidas;

4.204. Permitir o bloqueio de alterações, no caso acesso simultâneo de dois ou mais administradores;

4.205. Permitir definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;

4.206. Permitir autenticação integrada ao Microsoft Active Directory, servidor Radius, Novell eDirectory, LDAP e base de dados local, preferencialmente sem a necessidade de instalação ou utilização de nenhum software servidor, agente ou cliente. No caso da necessidade de instalação ou utilização de software adicional em servidor ou cliente, os dispositivos (de hardware e software) adicionais deverão, necessariamente, serem fornecidos pela Contratada;

4.207. Permitir autenticação de dois fatores;

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

4.209. Atribuir sequencialmente um número a cada regra de firewall, NAT, QOS e regras de DOS;

4.210. Permitir a criação de regras que fiquem ativas em horário definido;

4.211. Permitir a criação de regras com data de expiração;

4.212. Permitir backup das configurações e rollback de configuração para a última configuração salva;

4.213. Suportar Rollback de Sistema Operacional para a última versão local;

4.214. Permitir upgrade via, TFTP e interface de gerenciamento;

4.215. Validar políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);

a) É permitido o uso de appliance externo para permitir a validação de políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);

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

4.217. Deve possibilitar a integração com a solução de correlação de eventos RSA Security Analitics, podendo esta, ser através de SYSLOG;

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

4.219. Ter a capacidade de gerar um relatório gráfico que permita visualizar as mudanças na utilização de aplicações na rede no que se refere a um período de tempo anterior, para permitir comparar os diferentes consumos realizados pelas aplicações no tempo presente com relação ao passado;

4.220. Gerar relatórios com visualização das conexões discriminadas por países de origem e/ou destino, gerados em tempo real para a visualização de origens e destinos do tráfego;

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

4.222. Possibilitar a coleta de estatísticas de todo o tráfego que passar pelos dispositivos de segurança;

4.223. Possuir relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, Antivírus e Anti-Spware), etc;

4.224. Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus e Anti-Spware), e URLs que passaram pela solução;

4.225. Permitir navegação nos relatórios em tempo real, com identificação de acessos por usuário;

4.226. Ser possível exportar os logs em CSV;

4.227. Ser possível acessar o equipamento a aplicar configurações durante momentos onde o trafego é muito alto e a CPU e memória do equipamento estiver totalmente utilizada.

4.228. Possuir rotação de log;

4.229. Exibir as seguintes informações, de forma histórica e/ou em tempo real:

a) Situação do dispositivo e do cluster;
b) Principais aplicações;
c) Usuários autenticados na gerência da plataforma;
d) Número de sessões simultâneas;
e) Status das interfaces;
f) Uso de CPU;

4.230. Permitir a geração de no mínimo os seguintes relatórios:

a) Resumo gráfico de aplicações utilizadas;

b) Principais aplicações por utilização de largura de banda de entrada e saída;

c) Principais aplicações por taxa de transferência de bytes;

d) Principais hosts por número de ameaças identificadas;

e) Atividades de um usuário específico e grupo de usuários, incluindo aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças (IPS, Antivírus e Anti-Spware), de rede vinculadas a este tráfego;

4.231. Deve permitir a criação de relatórios personalizados;

4.232. Em cada critério de pesquisa do log deve ser possível incluir múltiplas entradas (ex. redes e IP's distintos; serviços HTTP, HTTPS e SMTP), exceto no campo horário, onde deve ser possível definir um faixa de tempo como critério de pesquisa;

4.233. Permitir gerar alertas automáticos via: Email, SNMP e Syslog;

4.234. Permitir a criação de regras e perfis baseadas em pré-existentes através da interface gráfica

4.235. O dispositivo para coleta e armazenamento de logs poderá ser fornecido de forma única, sem necessidade de equipamento redundante.

5. ADEQUAÇÃO ORÇAMENTÁRIA

Os recursos dessa contratação estão consignados no orçamento da União para 2016 no Programa 2100.8010.0001, Ação 8010, Fonte 0100, Elemento Contábil **3.3.9.0.39.27 – SUPORTE DE INFRAESTRUTURA DE TI.**

6. GARANTIA DOS SERVIÇOS

Os serviços da solução estarão cobertos por um Acordo de Nível de Serviço (SLA), com descontos na fatura mensal na ocorrência de descumprimento dos quesitos estabelecidos a seguir.

A contratada deverá disponibilizar consultas online, cujos resultados permitam a verificação da conformidade com o estabelecido no Acordo de Nível de Serviço (SLA), bem como o planejamento de capacidade e a análise da efetividade da solução. As consultas deverão permitir a seleção de períodos de abrangência, com possibilidade de exportação para arquivos HTML ou PDF. Pelo menos as seguintes informações deverão estar disponíveis:

- Data e hora de abertura da solicitação, identificação do solicitante, código de identificação da solicitação, descrição da solicitação, andamento da solicitação (worklog), data e hora de fechamento da solicitação; para todas as solicitações de alterações e inclusões de novas políticas, regras e filtros;
- Data e hora de registro do incidente, identificação do responsável pelo registro, código de identificação do incidente, descrição do incidente, severidade do incidente, data e hora da notificação do incidente e tratamento adotado para o incidente;
- Bloqueios efetuados pelo serviço de *firewall*;
- Bloqueios efetuados pelo serviço de filtragem de conteúdo, categorizados por tipo de conteúdo;
- Bloqueios feitos pelo serviço de prevenção de intrusão, totalizados por assinatura e/ou por endereços IP de origem e de destino;
- Endereços IP de origem e de destino com maior número de acessos, endereços IP de origem e de destino cujos acessos produziram o maior volume de tráfego;
- Volume de tráfego por protocolo;
- Disponibilidade diária dos equipamentos;
- Utilização de CPU, de memória RAM e tráfego nas interfaces de rede, aferidos em dias úteis, no período de 12h00 às 20h00;
- Taxa de ocupação de espaço em disco, se os equipamentos dispuserem deste recurso, aferidos em dias úteis, no período de 12h00 às 20h00;

Abaixo seguem os valores mensais de descontos em função de descumprimento do Acordo de Nível de Serviço (SLA), discriminados por item do acordo.

6.1. Disponibilidade dos Serviços

O percentual mínimo aceitável de disponibilidade mensal de todos os serviços que compõem a solução de segurança é de 99,7%. A disponibilidade corresponde ao percentual de tempo, durante um período de 30 dias de operação, em que todos os serviços da solução estiveram em condições normais de funcionamento.

Mensalmente, deverá ser calculado o percentual de disponibilidade da solução de segurança de perímetro, com base na seguinte fórmula:

D = [(43200–Ti)/43200]*100, onde:

- D= Percentual de disponibilidade
- Ti= Somatório dos minutos em que foram observadas inoperâncias em quaisquer dos serviços contemplados pela solução de segurança de perímetro durante o período de faturamento (30 dias).

Sempre que forem apurados percentuais de disponibilidade que estejam abaixo do limite mínimo estabelecido (99,7%), os somatórios dos tempos de inoperância, dentro do período de faturamento, serão descontados dos valores mensais da solução, tomando-se como base a seguinte fórmula:

Dc = (Vm*Ti)/43200, onde:

- Dc= Valor do desconto
- Vm= Valor mensal da solução.
- Ti= Somatório dos minutos em que foram observadas inoperâncias em quaisquer dos serviços contemplados pela solução de segurança de perímetro durante o período de faturamento (30 dias).

Ficam também estabelecidos limites de tolerância para os percentuais de disponibilidade calculados, que ao serem excedidos, determinarão glosas específicas nos valores da solução, conforme demonstrado a seguir:

- Percentuais de disponibilidade inferiores a 90% ensejarão a glosa de 50% do valor mensal da solução;
- Percentuais de disponibilidade inferiores a 80% ensejarão a glosa de 100% do valor mensal da solução.

Nos casos em que forem efetuadas as glosas acima (50% e 100%), não se aplicará o desconto no valor mensal calculado pela fórmula "Dc = (Vm*Ti)/43200".

6.2. Desempenho dos Equipamentos

Os equipamentos destinados à execução dos serviços deverão manter uma média semanal de uso de cada recurso computacional (CPU, memória RAM, tráfego nas interfaces de rede e taxa de utilização de espaço em disco) que não ultrapasse 70%, aferidos em dias úteis, no período de 12h00 às 20h00.

Sempre que um dos limites de desempenho dos equipamentos for ultrapassado, sem que tenha havido alterações nos parâmetros de rede estabelecidos, a contratada deverá promover a adequação ou reconfiguração do equipamento em um prazo máximo de 10 (dez) dias corridos.

A partir do primeiro dia de atraso, será suspenso o pagamento do valor relativo a cada dia da solução de segurança de perímetro, desde o momento em que o limite de desempenho foi ultrapassado até o retorno aos limites de desempenho estabelecidos.

6.3. Serviços em Regime de Alta Disponibilidade

Tendo em vista que a operação dos serviços da solução é suportada por equipamentos redundantes, em caso de falha de funcionamento de um dos equipamentos a contratada deverá realizar o reparo em até 72 (setenta e duas) horas, contadas a partir do momento da ocorrência da paralisação. Após esse prazo, será aplicada a regra estabelecida no item 7.1 Disponibilidade dos Serviços (Dc = (Vm*Ti)/43200), considerando que "Ti" será o tempo total, em minutos, de indisponibilidade do equipamento, contados a partir da falha de funcionamento.

6.4. Inclusão e/ou alteração de políticas, regras e filtros

As solicitações de alterações e inclusões de novas políticas, regras e filtros deverão ser efetivamente implementadas em um prazo máximo de 1 (uma) hora. A partir do início da segunda hora sem que a solicitação tenha sido atendida, e a cada período de 1 (uma) hora subseqüente, será aplicado o desconto de 1% sobre o valor mensal da solução.

6.5. Notificação de Incidentes

Para os incidentes que ensejarem obrigação da contratada de notificar o contratante, ou seja, para os quais não há um tratamento automático definido, esta notificação deverá ocorrer em um prazo máximo de 15 (quinze) minutos. A partir do primeiro minuto de atraso, e a cada período de 15 (quinze) minutos de atraso subseqüente, será aplicado o desconto de 1/30 sobre o valor mensal da solução.

6.6. Disponibilidade de Relatórios de Operação e Gestão

O percentual mínimo aceitável de disponibilidade mensal de todos os relatórios de operação e gestão é de 99,0%. A disponibilidade corresponde ao percentual de tempo, durante um período de 30 dias, em que todos os relatórios de operação e gestão estiveram acessíveis e com informações que refletiam a realidade.

Mensalmente, deverá ser calculado o percentual de disponibilidade dos relatórios de operação e gestão, com base na seguinte fórmula:

D = [(43200–Ti)/43200]*100, onde:

- D= Percentual de disponibilidade

- Ti= Somatório dos minutos em que foram observadas indisponibilidades em quaisquer relatórios de operação e gestão da solução de segurança de perímetro durante o período de faturamento (30 dias).

Sempre que forem apurados percentuais de disponibilidade dos relatórios que estejam abaixo do limite mínimo estabelecido (99,0%), os somatórios dos tempos de indisponibilidade, dentro do período de faturamento, serão descontados dos valores mensais da solução, tomando-se como base a seguinte fórmula:

Dc = (Vm*Ti)/43200, onde:

- Dc= Valor do desconto
- Vm= Valor mensal da solução.
- Ti= Somatório dos minutos em que foram observadas indisponibilidades em quaisquer dos relatórios de operação e gestão da solução de segurança de perímetro durante o período de faturamento (30 dias).

Ficam também estabelecidos limites de tolerância para os percentuais de disponibilidade calculados, que ao serem excedidos, determinarão glosas específicas nos valores da solução, conforme demonstrado a seguir:

- Percentuais de disponibilidade inferiores a 90% ensejarão a glosa de 50% do valor mensal da solução;
- Percentuais de disponibilidade inferiores a 80% ensejarão a glosa de 100% do valor mensal da solução.

Nos casos em que forem efetuadas as glosas acima (50% e 100%), não se aplicará o desconto no valor mensal calculado pela fórmula "Dc = (Vm*Ti)/43200".

6.7. Planilha Síntese do Acordo de Nível de Serviço (SLA) e das Penalidades

A PLANILHA SÍNTESE DE ACORDO DE NÍVEL DE SERVIÇOS E DE PENALIDADES representa uma síntese do Acordo de Nível de Serviço (SLA) e das penalidades às quais estará sujeita a contratada por descumprimento das exigências estabelecidas na presente especificação.

Para cada um dos itens de SLA da planilha, fica definido que ocorrerá um descumprimento parcial de contrato a cada 3ª (terceira) reincidência da aplicação de um desconto durante o contrato.

Para cada item, caso seja registrado um 2º (segundo) descumprimento parcial de contrato, será aplicada a multa prevista na planilha em dobro, percentual que será cobrado também para cada descumprimento parcial de contrato subsequente ao 2º (segundo).

Os descontos por descumprimento do Acordo de Nível de Serviço (SLA) são automáticos, mas a aplicação de multa por "descumprimento parcial de contrato" será sempre precedida de comunicação formal do contratante e amplo direito de defesa para a contratada.

PLANILHA SÍNTESE DE ACORDO DE NÍVEL DE SERVIÇOS E DE PENALIDADES

ITEM	SLA	Forma de Medição	Prazo Máximo/Limite Mínimo	Cálculo do Desconto	Limites de Tolerância	% Multa por Descumprimento Parcial
1	Disponibilidade dos Serviços.	Percentual de Tempo (Disponibilidade) D=[(43200–Ti)/43200]*100, onde: D= Percentual de disponibilidade Ti= Somatório dos minutos de inoperância observados durante o período de faturamento (30 dias).	2 (duas) horas/mês - 99,7%.	Dc=(Vm*Ti)/43200 Onde: Dc= Valor do desconto Vm= Valor mensal da solução Ti= Somatório dos minutos de inoperância observados durante o período de faturamento (30 dias).	D inferior a 90%: glosa de 50% do valor mensal. D inferior a 80%: glosa de 100% do valor mensal.	10,00%
2	Desempenho dos Equipamentos.	Prazo de adequação.	10 (dez) dias corridos para adequação dos equipamentos caso as médias semanais de uso de cada recurso computacional sejam superiores a 70%, aferidas em dias úteis, de 14:00 às 18:00 horas.	11/30 do valor mensal da solução para o 1° dia de atraso, acrescido de 1/30 para cada dia adicional.	----	10,00%
3	Serviços em Regime de Alta Disponibilidade.	Percentual de Tempo (Disponibilidade) D=[(43200–Ti)/43200]*100, onde: D= Percentual de disponibilidade Ti= Somatório dos minutos de inoperância do equipamento observados durante o período de faturamento (30 dias).	72 (setenta e duas) horas.	Dc=(Vm*Ti)/43200 Onde: Dc= Valor do desconto Vm= Valor mensal da solução Ti= Somatório dos minutos de inoperância do equipamento observados durante o período de faturamento (30 dias).	----	10,00%
4	Inclusão e/ou alteração de políticas, regras e filtros.	Prazo de inclusão/alteração.	1 (uma) hora.	1% do valor mensal da solução para cada hora de atraso.	----	5,00%

5	Notificação de Incidentes.	Prazo de notificação.	15 (quinze) minutos.	1/30 do valor mensal da solução para cada 15 (quinze) minutos de atraso.	----	10,00%
6	Disponibilidade de Relatórios	Percentual de Tempo (Disponibilidade) D=[(43200–Ti)/43200]*100, onde: D= Percentual de disponibilidade Ti= Somatório dos minutos de indisponibilidade observados durante o período de faturamento (30 dias).	7,2 (sete vírgula duas) horas/mês - 99,0%.	Dc=(Vm*Ti)/43200 Onde: Dc= Valor do desconto Vm= Valor mensal da solução Ti= Somatório dos minutos de indisponibilidade observados durante o período de faturamento (30 dias).	D inferior a 90%: glosa de 50% do valor mensal. D inferior a 80%: glosa de 100% do valor mensal.	10,00%

7. DAS PENALIDADES

7.1. Com fulcro no artigo 7º da Lei 10.520/2002 e artigos 86 e 87 da Lei nº 8.666/1993, a Administração poderá, garantida a prévia defesa, aplicar aos licitantes e/ou adjudicatários as seguintes penalidades, sem prejuízo das responsabilidades civil e criminal:

a) Advertência.

b) Multa, recolhida no prazo máximo de 5 (cinco) dias corridos, a contar da comunicação oficial, nas seguintes hipóteses:

- 0,3% (zero vírgula três por cento) por dia de atraso injustificado e por descumprimento das obrigações contratadas, até o máximo de 10% (dez por cento) sobre o valor total do Contrato;
- 10% (dez por cento) sobre o valor total contratado, no caso de inexecução total e 5% (cinco por cento) sobre o valor total contratado, no caso de inexecução parcial do objeto contratado.
- percentuais previstos na Planilha Síntese do Acordo de Nível de Serviço (SLA) e das Penalidades.

c) Impedimento de licitar e contratar com a União e descredenciamento do SICAF, pelo prazo de até 5 (cinco) anos, do licitante que não celebrar o contrato, deixar de entregar ou apresentar documentação falsa exigida para o certame, ensejar o retardamento da execução de seu objeto, não mantiver a proposta, falhar ou fraudar na execução do contrato, comportar-se de modo inidôneo ou cometer fraude fiscal.

d) Declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida sua reabilitação perante a própria autoridade que aplicou a penalidade.

7.2. O valor da multa, aplicada após o regular processo administrativo, poderá ser descontado dos pagamentos eventualmente devidos pela Administração à adjudicatária, acrescido de juros moratórios de 1% (um por cento) ao mês, ou cobrado judicialmente;

7.3. As sanções previstas nas alíneas "a", "c", e "d" do subitem 7.1. poderão ser aplicadas, cumulativamente ou não, à penalidade de multa da alínea "b".

7.4. As penalidades previstas neste capítulo obedecerão ao procedimento administrativo previsto na Lei 8.666/97, aplicando-se, subsidiariamente, a Lei 9.784/99.

7.5. Os recursos, quando da aplicação das penalidades previstas nas alíneas "a", "b", "c" e "d" do item 7.1 poderão ser interpostos no prazo máximo de 5 (cinco) dias úteis, a contar da intimação do ato ou da lavratura da ata.

7.6. No caso das penalidades previstas no item 7.1, alínea "d", caberá pedido de reconsideração ao Secretário-Geral do CNMP, no prazo de 10 (dez) dias úteis a contar da intimação do ato.

8. LOCAL DA PRESTAÇÃO DOS SERVIÇOS E IMPLANTAÇÃO

Os serviços de deverão ser prestados na Sede do CNMP, no Setor de Administração Federal Sul - SAFS, Quadra 2, Lote 3, CEP 70070-600 em Brasília-DF. Em caso de mudança da Sede do CNMP para outro local em Brasília-DF, a qualquer tempo, a empresa deverá prestar os serviços previstos neste projeto básico na nova sede e terá um prazo de 48 horas corridas para desinstalar os equipamentos da sede de origem e instalá-los na nova sede, deixando todos os serviços da solução plenamente funcionais e nas mesmas condições anteriores à migração, sem ônus adicionais para o CNMP

A entrega, a instalação e as configurações dos equipamentos serão de inteira responsabilidade da contratada.

A contratada deverá fornecer todos os materiais necessários à instalação física, à configuração e ao perfeito funcionamento dos equipamentos, incluindo rack, cabos elétricos e cabos lógicos. Caberá ao contratante o provimento das tomadas de alimentação elétrica e das portas para conexão à rede local.

A contratada deverá iniciar os serviços na Sede do CNMP em até 60 (sessenta) dias após a assinatura do contrato. Em reunião entre os gestores do contratante e os representantes da contratada, a ser realizada em até 30 (trinta) dias após a assinatura do contrato, deverão ser apresentados pela contratada:

- Sugestão de conjunto de políticas, regras e filtros a serem configurados nos serviços da solução de segurança de perímetro;
- Sugestão de graus de classificação de severidade de incidentes e as respectivas medidas que sugere serem adotadas em resposta aos alertas emitidos pelos serviços administrados;

As sugestões deverão ser apresentadas para discussão durante a reunião e também em documento detalhado, a ser entregue ao final da reunião, em mídia digital.

Em até 45 (quarenta e cinco) dias após a assinatura do contrato, deverá ocorrer nova reunião entre os gestores do contratante e os representantes da contratada, na qual os gestores do contratante apresentarão:

- O conjunto de políticas, regras e filtros que deverá ser configurado;
- Os nomes, telefones e demais informações para cadastramento de seus servidores que estarão encarregados de solicitar as implementações e alterações de políticas, regras e filtros;
- Os nomes, telefones e demais informações para cadastramento de seus servidores que serão os detentores das contas de acesso privilegiado à administração centralizada da solução;
- Os graus de classificação de severidade de incidentes e as respectivas medidas que deverão ser adotadas em resposta aos alertas emitidos pelos serviços administrados; e os nomes, telefones e demais informações para cadastramento de seus servidores que deverão ser notificados em caso de incidentes de determinado grau de severidade.

O contratante deverá manter o documento citado anteriormente atualizado durante toda a vigência do contrato, contendo todas as configurações lógicas e físicas (base de conhecimento), atualizando-o a cada implementação de alterações em políticas, regras, filtros , dentre outras ou em caso de alteração dos graus de classificação de severidade de incidentes e respectivas medidas de resposta, devendo este estar disponível para a CONTRATADA a qualquer tempo.

A contratada somente poderá dar início ao faturamento da solução após estar de posse do Termo de Recebimento dos Serviços, que será expedido pelo contratante em até 10 (dez) dias úteis após o término das instalações físicas e das configurações dos respectivos conjuntos de políticas, regras e filtros na Sede do CNMP, que deverá ocorrer no prazo máximo de 60 (sessenta) dias. A expedição do Termo de Recebimento dos Serviços também estará condicionada ao cumprimento integral de todos os requisitos estabelecidos.

9. VIGÊNCIA DO CONTRATO

O contrato terá vigência de 60 (sessenta meses) meses.

A execução do contrato iniciar-se-á com a implantação e efetivo funcionamento de todos os serviços especificados neste termo de referência que compõem a solução de segurança, o que deverá ocorrer em até 60 dias após a assinatura do contrato

10. PAGAMENTO

- O CONTRATANTE pagará à CONTRATADA, pelo fornecimento efetivamente executado, até o 10º (décimo) dia útil após o recebimento da Nota Fiscal/Fatura, devidamente atestada pelo Gestor do Contrato, por meio de depósito na conta corrente da CONTRATADA, através de Ordem Bancária, mediante apresentação da respectiva fatura ou nota fiscal do fornecimento, devidamente atestada pelo setor competente.
- Caso a CONTRATADA seja optante pelo "SIMPLES" (Lei nº 9.317/96), será obrigada a informar no corpo da nota fiscal e apresentar declaração, na forma do Anexo IV da Instrução Normativa SRF nº 1.234, de 11/01/2012, em duas vias, assinadas pelo seu representante legal.
- Para execução do pagamento de que trata a presente Cláusula, a CONTRATADA deverá fazer constar como beneficiário/cliente, da Nota Fiscal/Fatura correspondente, emitida sem rasuras, o **CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO, CNPJ nº 11.439.520/0001-11,** e ainda, o número da Nota de Empenho, os números do Banco, da Agência e da conta corrente da CONTRATADA e a descrição clara e sucinta do objeto.
- Sobre o valor da Nota Fiscal, a CONTRATANTE fará as retenções devidas ao INSS e as dos impostos e contribuições previstas na Instrução Normativa SRF nº 1.234, de 11/01/2012
- A CONTRATADA deverá, ainda, juntamente com a Nota Fiscal / Fatura, apresentar os documentos comprobatórios de regularidade fiscal e trabalhista, exigidos no Edital de Licitação.
- Nenhum pagamento será efetuado à CONTRATADA, enquanto pendente de liquidação qualquer obrigação financeira que lhe for imposta, em virtude de penalidade ou inadimplência contratual, sem que isso gere direito a acréscimos de qualquer natureza.
- Ao CONTRATANTE fica reservado o direito de não efetuar o pagamento se, no momento da aceitação, os serviços prestados, não estiverem em perfeitas condições e em conformidade com as especificações estipuladas.

11. OBRIGAÇÕES DA CONTRATANTE

Constituem obrigações do CONTRATANTE:

- Prestar as informações e esclarecimentos necessários ao desenvolvimento do objeto contratado;
- Relacionar-se com a CONTRATADA, exclusivamente, por meio de pessoa por ela formalmente indicada
- Assegurar o livre acesso do pessoal autorizado pela CONTRATADA, quando devidamente identificados e/ou uniformizados, ao local de entrega dos produtos;
- Exercer a fiscalização dos serviços contratados;
- Exigir, a qualquer tempo, a comprovação das condições de habilitação da CONTRATADA que ensejaram sua contratação, notadamente no tocante à qualificação econômico-financeira;
- Cumprir e fazer cumprir o disposto nas cláusulas deste Contrato, podendo aplicar as penalidades previstas na legislação vigente;
- Atestar o recebimento do objeto contratual por meio do Gestor competente;
- Efetuar, com pontualidade, os pagamentos à CONTRATADA, após o cumprimento das formalidades contratuais e legais;
- O CONTRATANTE, reserva-se o direito de exercer, quando lhe convier, fiscalização sobre os serviços contratados, e ainda, aplicar as penalidades previstas neste instrumento ou rescindi-lo, caso a CONTRATADA descumpra quaisquer das cláusulas estabelecidas;
- Será(ão) nomeado(s) Gestor(es) / Fiscais do Contrato, que será(ão) responsável(eis) pela fiscalização e acompanhamento da execução do objeto contratado, devendo fazer anotações e registros de todas as ocorrências, determinando o que for necessário à regularização das falhas ou defeitos observados para o fiel cumprimento das cláusulas e condições estabelecidas, e, ainda, atestar o recebimento do objeto;
- Os Gestores do Contrato terá(ão) poderes para:
- Definir toda e qualquer ação de orientação, gerenciamento, controle e acompanhamento da execução do Contrato, fixando normas nos casos não especificados e determinando as providências cabíveis;
- Paralisar temporariamente a execução do Contrato, total ou parcialmente, sempre que julgar necessário, submetendo o caso à autoridade competente para decisão.

- Recusar os serviços e ou equipamentos que não atendam satisfatoriamente ao determinado no objeto do Contrato, sendo, neste caso, a CONTRATADA obrigada a adequá-los e entregá-los nas dependências do CONTRATANTE no prazo determinado pelo Gestor do Contrato.

12. OBRIGAÇÕES DA CONTRATADA

A CONTRATADA se obriga a cumprir fielmente o estipulado no presente Instrumento e, em especial:

12.1. Quanto aos serviços

a) Tomar todas as providências necessárias ao fiel fornecimento do software e à execução dos serviços objetos deste Projeto Básico;

b) Manter, durante o período de vigência do contrato, todas as condições exigidas para habilitação no certame;

c) Responsabilizar-se integralmente pelo fiel cumprimento dos serviços contratados, prestando todos os esclarecimentos que forem solicitados pelo gestor do CNMP, cujas reclamações se obriga a atender;

d) Prestar suporte técnico por telefone, por correio eletrônico, por acesso remoto e por portal na Internet, para os técnicos do CNMP, com número ilimitado de chamados;

e) Deverá o portal na Internet possibilitar a abertura, o fechamento e o acompanhamento de todos os chamados, mesmo aqueles abertos por outro meio, com acesso aos técnicos do CNMP previamente cadastrados;

f) Encaminhar mensalmente relatório com a situação de todos os chamados abertos nos 3 (três) meses anteriores ao mês de envio;

g) A empresa deverá encaminhar juntamente com a nota fiscal para ateste e pagamento do serviço, relatório de chamados com datas de abertura, fechamento e SLA, ja com os devidos descontos conforme tabela de SLA, constante neste Termo,

h) Todas as ações realizadas em atendimento aos chamados abertos, devem ser testados previamente pela equipe a fim de comprovar sua eficácia (liberação de regras, vpn, etc.) sendo a finalização do chamado atrelada a comprovação do acesso/liberação efetuada.

i) Todo chamado relativo a modificação de regra/política, deve ser retornado por email com, no mínimo, os seguintes dados: id da regra, modificações efetuadas, texto original da abertura do chamado, hora da abertura do chamado, resposta ao chamado, SLA associado;

j) Executar os serviços por meio de técnicos comprovadamente especializados;

k) Apresentar seus empregados trajados de forma apropriada, identificados com crachás da empresa, quando nas dependências do CNMP, obedecendo as suas normas internas, inclusive as de segurança;

l) Não transferir a outrem, no todo ou em parte, o objeto do Contrato, sem prévia e expressa anuência do CNMP;

m) Não caucionar ou utilizar o Contrato para qualquer operação financeira, sob pena de rescisão contratual;

n) Manter em sua base interna e armazenada de forma segura, documentação atualizada e internalizada quanto a plataforma e arquitetura de TI do CNMP sobre a qual realizará suas operações assim como cópia das configurações dos dispositivos utilizados na solução. A fim de tornar mais célere e efetiva toda atuação, a equipe técnica da CONTRATADA, responsável pelos atendimentos referentes às demandas do Conselho, deverá ter conhecimento prévio do ambiente/arquitetura sobre a qual atuará. Este documento poderá ser solicitado a qualquer momento, de forma intempestiva ou não, pela equipe técnica do CNMP a fim de validar a documentação, devendo este ser entregue em até no máximo um dia após a sua requisição.

o) Manter e armazenar de forma segura e preferencialmente como referência de consulta rápida (registro no próprio equipamento, por exemplo) documentação atualizada e internalizada relativa a todas as regras, políticas e configurações realizadas/implementadas, ficando facultado a equipe técnica do Conselho, o pedido de emissão de relatório específico com estas informações.

p) Documentar, em campo próprio, quando disponível no equipamento, todas as regras contendo no mínimo: breve descrição, ID do chamado;

q) À CONTRATADA caberá realizar o planejamento, procedimentos e ações necessários para migração das regras, políticas, rotas, acessos, VPNs e usuários da plataforma que se encontra atualmente em operação na rede do CNMP para a solução instalada, assim como todas as configurações que se fizerem necessárias pra manutenção em operação de todos dos serviços utilizados e providos pelo Conselho naquilo que concerne a esta Solução. Esta implementação

deverá ser realizada com acompanhamento e aprovação da equipe técnica do CNMP e deverá ter também como premissa mitigar os possíveis impactos aos serviços e usuários do Conselho.

r) A CONTRATADA deverá manter serviço pró-ativo de gerencia e administração dos dispositivos envolvidos na solução, mantendo sempre atualizada as versões de software/firmware e monitorando os parâmetros e indicadores, necessários para o perfeito funcionamento da solução de forma a mitigar os riscos de segurança e ocorrência de falhas.

s) Deverá disponibilizar, para consulta online, com possibilidade de análise em tempo real, todos os registros referentes à acesso ao equipamento, IPS, IDS, acesso VPN, acessos à internet, redes internas e servidores, dentre outras informações pertinentes para fins de auditoria e/ou verificação de acessos e efetividade de configurações, pelo prazo mínimo de 2 meses. Após este período os registros deverão ser armazenados de forma off-line para consulta durante toda a vigência contratual.

12.2. Quanto aos empregados

a) Orientar seus empregados para que se comportem sempre de forma cordial e urbana;

b) Zelar para que seus empregados se mantenham devidamente identificados por meio de crachás de identificação sempre que estiverem circulando nas dependências do CONTRATANTE;

c) Substituir qualquer empregado, no prazo máximo de 24 (vinte e quatro horas), cuja atuação, permanência e/ou comportamento sejam julgados prejudiciais, inconvenientes e/ou insatisfatórios pelo Gestor do Contrato;

12.3. Quanto às vedações

a) Não ter como sócios, gerentes, diretores ou administradores cônjuges, companheiros(as) ou parentes em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, de membros e servidores ocupantes de cargos de direção, chefia ou assessoramento do Conselho Nacional do Ministério Público, sob pena de rescisão contratual;

b) Não reproduzir, divulgar ou utilizar em benefício próprio, ou de terceiros, quaisquer informações de que tenha tomado ciência em razão da execução dos serviços discriminados, sem o consentimento prévio e por escrito do CONTRATANTE;

c) Não permitir que seus empregados pratiquem a venda de quaisquer mercadorias e produtos nas dependências do CONTRATANTE, bem como que executem atividades incompatíveis com as previstas neste Contrato;

d) Não utilizar o nome do CONTRATANTE, ou sua qualidade de CONTRATADA, em quaisquer atividades de divulgação empresarial, como, por exemplo, em cartões de visita, anúncios e impressos, sem o consentimento prévio e por escrito do CONTRATANTE;

e) Não transferir a outrem, no todo ou em parte, o objeto do presente Contrato, sem prévia e expressa anuência do CONTRATANTE;

f) Não caucionar ou utilizar o Contrato para quaisquer operações financeiras, sob pena de rescisão contratual.

g) Não divulgar, sob qualquer pretexto, as características dos sistemas, equipamento(s), elemento(s) e instalação(ões), bem como outras informações que porventura venha a ter acesso, em função do desempenho das suas atividades.

12.4. Quanto à responsabilidade empresarial

a) Responsabilizar-se pelos danos causados ao patrimônio do CONTRATANTE, por dolo ou culpa de seus empregados, ficando obrigada a promover a devida restauração e/ou o ressarcimento a preços atualizados, dentro de 30 (trinta) dias contados a partir da comprovação de sua responsabilidade. Caso não o faça no prazo estipulado, o CONTRATANTE reserva-se o direito de descontar o valor do ressarcimento na fatura do mês, e/ou da garantia, sem prejuízo de poder denunciar o Contrato, de pleno direito.

b) Responsabilizar-se integralmente pelo fiel cumprimento dos serviços contratados, prestando todos os esclarecimentos que lhe forem solicitados pelo CONTRATANTE, cujas reclamações se obriga a atender;

12.5. Quanto às obrigações gerais

a) Manter, as condições de habilitação e qualificação que ensejaram a contratação durante a execução do Contrato;

b) Disponibilizar uma conta de e-mail para fins de comunicação entre as partes;

c) Manter atualizados o endereço comercial, de e-mail e os números de telefone e de fax.

13. PROPOSTA

- A proposta apresentada deverá conter o CNPJ da proponente, prazo de validade e ser endereçada ao Conselho Nacional do Ministério Público – CNMP.
- Nos preços da proposta deverão estar inclusas todas as despesas e custos diretos e indiretos, como impostos, taxas e fretes.
- A proposta deverá conter marca e modelo dos equipamentos que darão suporte aos serviços;
- As proponentes deverão apresentar preço mensal e total, conforme quadro abaixo:

Descrição	**Valor Mensal (R$)**
Solução de Segurança	-
Valor Global da Solução (Valor Mensal x 60)*	-

Será considerada vencedora a proposta que apresentar o menor Valor Global da Solução.

*Observação: O Valor Global da Solução foi estipulado em 60 (sessenta) meses considerando-se a vigência contratual e que a Contratada poderá iniciar a execução do contrato antes do prazo máximo de 60 (sessenta) dias, nos termos do item DA VIGÊNCIA DO CONTRATO.

14. CRITÉRIOS DE QUALIFICAÇÃO TÉCNICA EXIGIDOS PARA A CONTRATADA

Para habilitação no certame a empresa deverá apresentar no mínimo 1 (um) atestado que comprove aptidão técnica, expedido por pessoa jurídica de direito público ou privado. O documento deve comprovar que a licitante forneceu ou fornece serviço de SNOC *(Security Network Operation Center)*, contemplando administração remota, monitoramento reativo e proativo em regime 24x7x365, com fornecimento de solução composta de pelo menos solução de firewall, detecção e prevenção de intrusão (IPS/IDS), filtro de conteúdo, mail relay, antispam, antivírus de rede e email e VPN *(Virtual Private Network)*..

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

Poderá haver teste de bancada para comprovar a conformidade dos dispositivos oferecido caso a instituição julgue necessário, através de amostra dos equipamentos.

- Caso a instituição solicite amostra da solução, a licitante deverá fornecer amostra dos equipamentos para que seja verificado o atendimento aos itens do edital, incluindo a capacidade do equipamento e as funcionalidades exigidas.
- A proponente deverá fornecer todos os equipamentos para geração de tráfego de acordo com as solicitações de performance descritas neste edital sem custo para a instituição;
- O teste de bancada poderá aferir o desempenho dos equipamentos como as funcionalidades que fazem uso de assinaturas, habilitadas para todas as assinaturas que a plataforma de segurança possuir, bem como amostra de todos os recursos solicitados;
- Os testes deverão ser executados nas dependências da sede da instituição em um prazo máximo de 30 dias após a solicitação da amostra;
- A amostra deverá ser identificada com o número da licitação, o objeto, o nome do licitante, seu telefone e endereço.
- A amostra aprovada ficará retida para confronto com os materiais, quando do seu recebimento pela instituição.
- A instituição se reserva o direito de não aceitar a amostra, independentemente da informação contida na proposta em relação à marca, caso não atenda às especificações exigidas, ou seja, de qualidade inferior à dos materiais solicitados.
- Amostras não aprovadas permanecerão à disposição dos respectivos licitantes, para retirada, pelo prazo de 90 (noventa) dias úteis após a conclusão do processo licitatório. As amostras não retiradas serão descartadas pela instituição.
- Será emitido um relatório sucinto descrevendo os exames realizados e contendo a aprovação ou não do material/produto.

Para as funcionalidades técnicas referentes aos equipamentos que irão compor a solução, o for-

necedor deverá apresentar Tabela de Comprovação Técnica, conforme modelo abaixo, a qual deve ser entregue junto a proposta comercial;

- A Contratada deverá apresentar tabela preenchida, composta de todos os itens técnicos contidos neste edital que especificam funcionalidades dos dispositivos que irão compor a solução, incluindo apresentação de documentação com indicação da página, onde deve se encontrar grifadas as comprovações de cada uma das funcionalidades e características exigidas;
- A Tabela de Comprovação Técnica deve conter, ainda, nome do documento comprobatório emitido pelo Fabricante;

N.° do Item	Descrição da Característica/ Funcionalidade Exigida	Documento do Fabricante (Nome)	Página(s)	Atende ao Requisito (Sim/Não)
1.	.....	.....	.....	.....
1.1.	.....	.....	.....	.....

- Serão considerados documentos oficiais para comprovação técnica: catálogos, folders, prospectos e manuais;
- Todos os documentos devem estar completos e legíveis;
- No caso de alguma funcionalidade ou característica técnica exigida não se encontrar explicita nos documentos, será aceito declaração emitida pelo Fabricante afirmando o atendimento de tal característica ou funcionalidade;
- Os documentos técnicos fornecidos que não apresentarem numeração de página deverão ser numerados manualmente de forma visível pela Licitante, no canto inferior direito;
- Além da indicação da página da documentação fornecida onde se encontra a comprovação de cada funcionalidade ou característica técnica exigida para cada item, a correspondente comprovação deverá ser necessariamente grifada

15. PROPRIEDADE, SIGILO E RESTRIÇÕES

- A empresa contratada se comprometerá, por escrito, a manter sigilo acerca das informações obtidas e geradas no decorrer do contrato, mediante assinatura de Termo Confidencialidade e Compromisso com a Segurança da Informação, conforme modelo em anexo.

- Pertencerão exclusivamente ao Contratante os direitos relativos aos produtos desenvolvidos e elaborados especificamente sob demanda durante a vigência do Contrato, sendo vedada sua reprodução, transmissão ou divulgação sem o seu respectivo consentimento prévio.
- Durante a execução dos serviços, a Contratada deverá observar as Políticas de Controle de Acesso definidas pelo CNMP.
- Ao término do contrato, a Contratada se compromete a permitir o acesso a solução somente para leitura, em um prazo de até 30 (trinta) dias corridos para que a equipe técnica do CNMP possa transferir os dados armazenados na solução para outro ambiente e após esse prazo a Contratada se compromete a excluir, em até 30 (trinta) dias corridos, de qualquer mídia (on-line ou backup) definitivamente, sem possibilidade de recuperação, para quaisquer fins, todas as informações do CNMP armazenadas na solução durante a vigência do contrato.
- Ao término do contrato, a Contratada se compromete a enviar todas as informações do CNMP armazenadas na solução em meio eletrônico para que o CNMP possa guardar.
- Toda informação armazenada na solução deve ser criptografada para arquivamento e transmissão.
- Nenhuma informação pode ser compartilhada com terceiros, para quaisquer fins, ou utilizada para outros fins que não estejam associados diretamente à prestação dos serviços contratados.

16. DO RECEBIMENTO

O recebimento se dará, provisoriamente, no início da operação dos serviços, para posterior verificação da conformidade técnica em relação às características técnicas mínimas especificadas neste projeto básico.

A contratada somente poderá encaminhar faturas relativas à solução após estar de posse do Termo de Recebimento Definitivo dos Serviços, que será expedido pelo contratante em até 10 (dez) dias úteis após o término das instalações físicas e das configurações dos respectivos conjuntos de políticas, regras e filtros, o que deverá ocorrer no prazo máximo de 60 (sessenta) dias. A expedição do Termo de Recebimento Definitivo dos Serviços consignará a data a partir da qual os serviços poderão ser considerados implantados e sujeitos a faturamento, com base na data de averiguação do cumprimento integral de todos os requisitos estabelecidos.