



ESTADO DE MATO GROSSO  
SECRETARIA DE ESTADO DO MEIO AMBIENTE  
SECRETARIA ADJUNTA DE GESTÃO SISTÊMICA  
COORDENADORIA DE AQUISIÇÕES E CONTRATOS  
GERENCIA DE FORMALIZAÇÃO DE CONTRATOS

TERMO DE CONTRATO N°. 043/2014/SEMA QUE  
ENTRE SI CELEBRAM A SECRETARIA DE ESTADO  
DO MEIO AMBIENTE - SEMA E A EMPRESA FAST  
SECURITY TECNOLOGIA DA INFORMAÇÃO LTDA.

O ESTADO DE MATO GROSSO, através da SECRETARIA DE ESTADO DO MEIO AMBIENTE - SEMA, inscrita no CNPJ/MF sob o n.º 03.507.415/0023-50, criada pela Lei Complementar n.º. 214, de 23 de junho de 2005, com sede na Rua C, esquina com a Rua F, Palácio Paiaguás, Centro Político Administrativo - CPA, nesta Capital, representada pelo Secretário Adjunto de Gestão Sistêmica, Sr. **Benedito Nery Guarim Strobel**, brasileiro, casado, portador do RG n.º. 349.280 - SSP/MT e do CPF n.º. 298.940.931-91, residente a Rua Dom Antonio Malan, 756, Bairro Poção, CEP: 78.015-608, Cuiabá/MT, nomeado pelo Ato Governamental n.º 18.861/2014 de 26/02/14, doravante denominada apenas **CONTRATANTE** e de outro lado a empresa **FAST SECURITY TECNOLOGIA DA INFORMAÇÃO LTDA. ME**, inscrita no CNPJ 10.647.012/0001-66, localizada na Scia quadra 14, conjunto 03, lote 03, 1º andar, parte A - Guará, em Brasília-DF, CEP: 71.250-115, telefone: (61)3363-8636, representada pelo Sr. **GUSTAVO LIMA MIRANDA**, portador do RG 1.828.256 - SSP/DF e do CPF: 707.868.101-06, doravante denominada **CONTRATADA**, firmam o presente instrumento, em conformidade com o Processo n.º 468778/2014/SEMA, edital de **Pregão Eletrônico n.º 033/2013 - COLOG e Ata de Registro de Preços n.º 00001/2013 do Exército Brasileiro/Ministério da Defesa**, sujeitando-se aos termos da Lei n.º 8.666, de 21 de junho de 1993 e alterações posteriores, Lei n.º. 10.520/2002, Decreto Estadual n.º 7.217/2006, bem como, mediante as cláusulas e condições a seguir expressas:

**1. CLÁUSULA PRIMEIRA - DO OBJETO**

**1.1.** O presente contrato tem por objeto a contratação de empresa especializada para fornecimento de solução de segurança - IPS TIPO I, conforme especificações e condições descritas no **Pregão Eletrônico n.º 033/2013 - COLOG/Exército Brasileiro** e seus anexos, bem como, no Termo de Referência n.º 110/2014 elaborado pelo setor demandante, que fazem parte integrante deste contrato, independente de transcrição.



ESTADO DE MATO GROSSO  
SECRETARIA DE ESTADO DO MEIO AMBIENTE  
SECRETARIA ADJUNTA DE GESTÃO SISTÊMICA  
COORDENADORIA DE AQUISIÇÕES E CONTRATOS  
GERENCIA DE FORMALIZAÇÃO DE CONTRATOS

**2. CLÁUSULA SEGUNDA - DAS ESPECIFICAÇÕES, QUANTIDADES E PREÇO**

2.1. O preço para o objeto contratado é o constante da proposta apresentada, nos termos do edital de **Pregão Eletrônico n.º 033/2013 - COLOG/Exército Brasileiro** e seus anexos, conforme discriminação abaixo:

**LOTE ÚNICO**

ITEM	ESPECIFICAÇÃO DO ITEM	UNID	QTD	VALOR UNIT	VALOR TOTAL
03	Aquisição Complementar de nova Solução de IPS TIPO I a ser usado em alta disponibilidade integrado com solução já existente no ambiente da DFPC com garantia de manutenção e suporte para 36 Meses	SV	02	185.000,00	370.000,00
VALOR TOTAL					370.000,00

**Detalhamento do objeto**

Item ARP	Descrição	Qtde	Valor Unit.	Valor Total
03	Hardware - PA3020 CONTENDO SOFTWARE PAN-OS COM FILTRO DE URL E THREAT PREVENTION ATIVOS	02	81.554,00	163.108,00
	Serviço de Suporte/Garantia	01	90.000,00	90.000,00
	Serviço de Treinamento	05	10.000,00	50.000,00
	Serviço de Instalação	01	66.892,00	66.892,00
TOTAL				370.000,00

2.2. A **CONTRATANTE** pagará à **CONTRATADA**, pelo objeto ora contratado, o valor total de **R\$ 370.000,00** (trezentos e setenta mil reais), a serem pagos em parcela única, após a efetiva entrega do objeto, comprovada por meio de atesto do fiscal do contrato, designado pela **COORDENADORIA DE TECNOLOGIA DA INFORMAÇÃO DA CONTRATANTE**;

2.3. Os valores poderão eventualmente sofrer revisão (aumento ou decréscimos) nas seguintes hipóteses:



**ESTADO DE MATO GROSSO**  
**SECRETARIA DE ESTADO DO MEIO AMBIENTE**  
**SECRETARIA ADJUNTA DE GESTÃO SISTÊMICA**  
**COORDENADORIA DE AQUISIÇÕES E CONTRATOS**  
**GERENCIA DE FORMALIZAÇÃO DE CONTRATOS**

a) Para mais, visando restabelecer o equilíbrio econômico-financeiro inicial do contrato, na hipótese de sobrevir fatos supervenientes imprevisíveis, ou previsíveis, porém, de consequências incalculáveis, retardadores ou impeditivos da execução do ajustado, ou ainda, em caso de força maior caso fortuito, fato do príncipe e fato da administração, nos termos do art. 65, II, "d" e § 5º da Lei 8.666/93;

b) Para menos, na hipótese do valor contratado ficar muito superior ao valor do mercado, ou, ainda, quando ocorrer o fato do príncipe previsto no art. 65, § 5º da Lei 8.666/93.

**2.4.** A revisão de preços será feita com fundamento em planilhas de composição de custos e/ou preço de mercado;

**2.5.** Nos preços supracitados estão incluídas todas as despesas relativas ao objeto contratado (tributos, seguros, encargos sociais, etc.).

**3. CLÁUSULA TERCEIRA - DAS OBRIGAÇÕES DA CONTRATADA**

**3.1.** Assinar o contrato no prazo de **10 (dez) dias**, contados a partir do recebimento da convocação formal, bem como, retirar a Ordem de Fornecimento/Serviço a ser emitida pelo setor demandante.

**3.2.** Executar o fornecimento dentro dos padrões contratados e estabelecidos pela **CONTRATANTE**, de acordo com as especificações e condições constantes no Edital de **Pregão Eletrônico n.º 033/2013 - COLOG** e anexos, na **Ata de Registro de Preços n.º 00001/2013 do Exército Brasileiro/Ministério da Defesa** e proposta apresentada, responsabilizando-se por eventuais prejuízos decorrentes do descumprimento de condição estabelecida.

**3.3. Da Confidencialidade**

**3.3.1.** Os cuidados com a salvaguarda das informações dos produtos que representam o objeto deste contrato são responsabilidade da **CONTRATADA**,



ESTADO DE MATO GROSSO  
SECRETARIA DE ESTADO DO MEIO AMBIENTE  
SECRETARIA ADJUNTA DE GESTÃO SISTÊMICA  
COORDENADORIA DE AQUISIÇÕES E CONTRATOS  
GERENCIA DE FORMALIZAÇÃO DE CONTRATOS

conforme prevê o Decreto nº 4.553, de 27 de dezembro de 2002, nos seguintes artigos e parágrafos:

Art. 56. "A definição do meio de transporte a ser utilizado para deslocamento de material sigiloso é responsabilidade do detentor da custódia e deverá considerar o respectivo grau de sigilo."

§ 1º O material sigiloso poderá ser transportado por empresas para tal fim contratadas.

§ 2º As medidas necessárias para a segurança do material transportado serão estabelecidas em entendimentos prévios, por meio de cláusulas contratuais específicas, e serão de responsabilidade da empresa contratada.

Art. 65. "Toda e qualquer pessoa que tome conhecimento de documento sigiloso, nos termos deste Decreto fica, automaticamente, responsável pela preservação do seu sigilo." Continuação do edital do pregão eletrônico/SRP Nº 033/2013 - COLOG Página 81 de 84.

**3.3.2.** Cabe esclarecer que, de acordo com o amparo supracitado, a **CONTRATADA** será responsável por salvaguardar quaisquer informações relacionadas aos pedidos formulados pela Divisão de Tecnologia da Informação (DIVTI), dispensando especial atenção para a preservação de dados atinentes às áreas de interesses e às datas dos pedidos de aquisição das imagens.

**3.4.** Assumir inteira responsabilidade pela entrega do objeto contratado.

**3.5.** Executar o objeto contratado de acordo com as especificações, não sendo aceitas quaisquer modificações sem a expressa autorização, por escrito, do Fiscal do Contrato.

**3.6.** Submeter à aprovação da **CONTRATANTE** toda e qualquer alteração ocorrida nas especificações, em face das imposições técnicas, de cunho administrativo, de implementos tecnológicos ou legais indispensáveis à perfeita execução dos serviços.

**3.7.** Sujeitar-se à fiscalização da **CONTRATANTE** no tocante à verificação das especificações técnicas, prestando os esclarecimentos solicitados,



ESTADO DE MATO GROSSO  
SECRETARIA DE ESTADO DO MEIO AMBIENTE  
SECRETARIA ADJUNTA DE GESTÃO SISTÊMICA  
COORDENADORIA DE AQUISIÇÕES E CONTRATOS  
GERENCIA DE FORMALIZAÇÃO DE CONTRATOS

atendendo às reclamações procedentes, caso ocorram, e prestando toda assistência técnica operacional.

**3.8.** Acatar todas as orientações do Fiscal do Contrato, sujeitando-se a mais ampla e irrestrita fiscalização, prestando os esclarecimentos sobre o objeto contratado e atendimento das reclamações formuladas.

**3.9.** Prestar garantia pelo prazo constante na cláusula Décima Nona do edital.

**3.10.** Responsabilizar-se por quaisquer danos ou prejuízos causados por seus empregados aos equipamentos, instalações, patrimônio e bens da **CONTRATANTE**, em decorrência da execução dos serviços, incluindo-se também os danos materiais ou pessoais a terceiros, a que título for. O **CONTRATANTE** estipulará o prazo para a reparação dos danos e prejuízos causados.

**3.11.** Manter disciplina nos locais de entrega do objeto contratado, retirando, de imediato, qualquer empregado cuja atuação, permanência e/ou comportamento seja considerados inconvenientes ou insatisfatórios ao interesse do Serviço Público.

**3.12.** Manter, durante a vigência deste contrato as condições de habilitação para contratar com a Administração Pública, apresentando, sempre que exigido, os comprovantes de regularidade fiscal.

**3.13.** Cuidar para que todos os privilégios de acesso a sistemas, informações e recursos da **CONTRATANTE** sejam revistos, modificados ou revogados quando da transferência, remanejamento, promoção ou demissão de profissionais sob sua responsabilidade, em casos de paralisação dos transportes coletivos, bem como nas situações nas quais se faça necessária a execução dos serviços em regime extraordinário.

**3.14.** A **CONTRATADA** cabe assumir a responsabilidade por:

**3.14.1.** Todos os encargos previdenciários e obrigações sociais previstos na legislação social e trabalhista em vigor, obrigando-se a saldá-los na



ESTADO DE MATO GROSSO  
SECRETARIA DE ESTADO DO MEIO AMBIENTE  
SECRETARIA ADJUNTA DE GESTÃO SISTÊMICA  
COORDENADORIA DE AQUISIÇÕES E CONTRATOS  
GERENCIA DE FORMALIZAÇÃO DE CONTRATOS

época própria, vez que os seus empregados não manterão nenhum vínculo empregatício com a **CONTRATANTE**;

**3.14.2.** Todas as providências e obrigações estabelecidas na legislação específica de acidentes de trabalho, quando em ocorrência da espécie, forem vítimas os seus empregados durante a execução deste contrato, ainda que acontecido em dependência da **CONTRATANTE**;

**3.14.3.** São expressamente vedadas à **CONTRATADA**:

**3.14.4.** A veiculação de publicidade acerca deste contrato, salvo se houver prévia autorização da Administração da **CONTRATANTE**;

**3.14.5.** A subcontratação de outra empresa para a execução do objeto deste contrato.

**3.14.6.** Comprovação da origem dos bens importados oferecidos, e da quitação dos tributos de importação a eles referentes, que deverá ser apresentado no momento da entrega do objeto, sob pena de rescisão contratual e multa;

**3.14.** Demais obrigações e responsabilidades previstas na Lei nº. 8.666/93 e alterações, Lei nº. 10.520/2002, Decreto Estadual nº. 7.217/2006, Edital de **Pregão Eletrônico n.º 033/2013 - COLOG** e anexos, e **Ata de Registro de Preços n.º 00001/2013 do Exército Brasileiro/Ministério da Defesa**.

#### **4. CLÁUSULA QUARTA - DO RECEBIMENTO E DA EXECUÇÃO DO OBJETO**

**4.1.** Os serviços objeto deste contrato serão considerados entregues, após a instalação e configuração dos mesmos e deverão ser instalados na COORDENADORIA DE TECNOLOGIA DA INFORMAÇÃO da **CONTRATANTE**, em até **45 (quarenta e cinco) dias** a partir do recebimento da Ordem de Fornecimento/Serviço emitida pelo setor demandante, correndo por conta da **CONTRATADA** todas as despesas decorrentes.



ESTADO DE MATO GROSSO  
SECRETARIA DE ESTADO DO MEIO AMBIENTE  
SECRETARIA ADJUNTA DE GESTÃO SISTÊMICA  
COORDENADORIA DE AQUISIÇÕES E CONTRATOS  
GERENCIA DE FORMALIZAÇÃO DE CONTRATOS

**4.1.1.** A **CONTRATADA** deverá agendar formalmente, com a COORDENADORIA DE TECNOLOGIA DA INFORMAÇÃO da **CONTRATANTE**, a data e o horário para a instalação do software, com antecedência mínima de 15 (quinze) dias, podendo utilizar-se de telefone para o contato.

**4.2.** A **CONTRATADA** será responsável pela substituição, troca ou reposição do (s) produto (s) se em até **15 (quinze) dias**, porventura, for (em) entregue (s) com qualquer natureza de defeito, avaria ou não compatíveis com as especificações deste contrato.

**4.2.1.** O fornecedor da solução realizará treinamento para utilização do produto, a ser ministrado nas dependências da **CONTRATANTE**, para no mínimo 05 (cinco) técnicos indicados pela Coordenadoria de Tecnologia da **CONTRATANTE**, com 12 (doze) horas de duração em data e horários a serem estabelecidos pela **CONTRATANTE**.

**4.2.2.** Serão observados os **prazos de garantia** dos serviços executados.

**4.3.** Após a instalação dos componentes da solução de antivírus, conforme as especificações técnicas, a Coordenadoria de Tecnologia da **CONTRATANTE** confeccionará o Termo de Recebimento Definitivo (TRD) acompanhado da nota fiscal original com atesto no verso, para fins de pagamento.

**4.4.** Em caso de NÃO conformidade com as especificações técnicas, a **CONTRATANTE** notificará a **CONTRATADA** para sanar os problemas ou para efetuarem a reposição de todo o material defeituoso **no prazo de 30 (trinta) dias**. Caso contrário, a **CONTRATADA** ficará sujeita as sanções administrativas por deixar de cumprir o estabelecido nas especificações técnicas do produto.

**4.5.** Caso a **CONTRATADA** indique que o objeto do contrato será procedente de país estrangeiro, a **CONTRATADA** deverá apresentar como condição obrigatória para o recebimento, a licença e a documentação aduaneira de liberação da importação, junto com a nota fiscal.

**4.6.** Será rejeitado, no todo ou em parte, o que for fornecido em desacordo com este contrato.



ESTADO DE MATO GROSSO  
SECRETARIA DE ESTADO DO MEIO AMBIENTE  
SECRETARIA ADJUNTA DE GESTÃO SISTÊMICA  
COORDENADORIA DE AQUISIÇÕES E CONTRATOS  
GERENCIA DE FORMALIZAÇÃO DE CONTRATOS

#### 4.7. Da Catalogação

4.7.1. A **CONTRATADA** obriga-se a apresentar, antes do fornecimento do material objeto principal do contrato, todos os dados técnicos de identificação do objeto deste contrato, para efeito de catalogação dos mesmos pelo Sistema de Catalogação da **CONTRATANTE**.

4.7.2. A **CONTRATADA** ficará obrigada a fornecer todos os dados técnicos necessários para a identificação dos itens de suprimento, para efeito de catalogação dos mesmos através do Sistema de Catalogação da **CONTRATANTE**, devendo incluir nome e endereço dos fabricantes ou fornecedores, número de desenho ou referência fabril, normas, especificações e desenhos técnicos, conforme o anexo "G" ao edital.

#### 4.8. Da Prorrogação do Prazo de Entrega

4.8.1. Os prazos de entrega poderão ser prorrogados, desde que ocorra um dos seguintes motivos:

- a) alteração das especificações pela contratante;
- b) superveniência de fato excepcional ou imprevisível, estranho à vontade das partes, que altere fundamentalmente as condições de execução deste contrato;
- c) interrupção da execução deste contrato ou diminuição do ritmo de trabalho por ordem e no interesse da contratante; 10.1.4. aumento das quantidades inicialmente previstas neste contrato em até **25 % (vinte e cinco por cento)** do seu valor inicial atualizado, conforme limites permitidos pelo art. 65 da Lei nº 8666/93, em sua redação atual;
- d) impedimento de execução deste contrato por ato ou fato de terceiro reconhecido pela contratante em documento contemporâneo a sua ocorrência; e
- e) omissão ou atraso de providências a cargo da **CONTRATANTE**, inclusive quanto aos pagamentos previstos de que resulte diretamente impedimento ou retardamento na execução deste contrato.
- f) Verificado algum dos motivos relacionados, a **CONTRATANTE** poderá conceder a prorrogação necessária, desde que o respectivo pedido seja apresentado pela **CONTRATADA** e, mediante petição por escrito, devidamente





**ESTADO DE MATO GROSSO  
SECRETARIA DE ESTADO DO MEIO AMBIENTE  
SECRETARIA ADJUNTA DE GESTÃO SISTÊMICA  
COORDENADORIA DE AQUISIÇÕES E CONTRATOS  
GERENCIA DE FORMALIZAÇÃO DE CONTRATOS**

fundamentado e protocolada no Protocolo-Geral da **CONTRATANTE**, até **dez dias** antes do vencimento do prazo contratual.

**4.9. Da comunicação**

**4.9.1.** Qualquer notificação, solicitação ou comunicação que as partes devam enviar uma à outra, em virtude deste contrato, será feita por escrito e considerar-se-á efetuada no momento em que o documento for entregue ao destinatário nos endereços indicados por ambas.

**5. CLÁUSULA QUINTA - DA GARANTIA CONTRATUAL**

**5.1.** No prazo máximo de até **30 (trinta) dias**, a partir da assinatura do contrato, a **CONTRATADA** deverá prestar a garantia correspondente a **5% (cinco por cento)** do valor total da contratação, em uma das modalidades previstas no art. 56, da Lei nº 8.666/93, com validade de no mínimo sessenta dias após a data limite prevista para o término da vigência deste contrato, devendo ser renovada a cada prorrogação efetivada no contrato.

**5.2.** A liberação da garantia prestada será feita, após o cumprimento integral deste contrato, comprovado pelo recebimento definitivo de seu objeto, por comunicação expressa da **CONTRATANTE**.

**5.3.** No caso de caução em dinheiro, o mesmo deverá ser realizado mediante depósito/transferência eletrônica, na conta e agência do Banco do Brasil abaixo informada:

**AG: 3834-2 BANCO DO BRASIL**

**C/C : 1.042.456-3**

**IDENT.: SEMA/CAUÇÃO**

**6. CLÁUSULA SEXTA - DA GARANTIA TÉCNICA**

**6.1.** A garantia dos produtos e da prestação dos serviços de suporte técnico será de 36 (trinta e seis) meses, contados a partir da data de



ESTADO DE MATO GROSSO  
SECRETARIA DE ESTADO DO MEIO AMBIENTE  
SECRETARIA ADJUNTA DE GESTÃO SISTÊMICA  
COORDENADORIA DE AQUISIÇÕES E CONTRATOS  
GERENCIA DE FORMALIZAÇÃO DE CONTRATOS

emissão do Termo de Recebimento definitivo. Podendo ser prorrogada de acordo com a vigência contratual.

6.2. A garantia deverá englobar qualquer atividade relacionada ao funcionamento dos produtos, como manutenção evolutiva, preventiva e corretiva em hardware e software, sem nenhum ônus para a **CONTRATANTE**.

6.3. Durante o período de garantia é de responsabilidade da **CONTRATADA**, a atualização de versões dos softwares e hardwares fornecidos, mesmo que saiam de linha e não sejam mais suportados pelo fabricante.

6.4. A **CONTRATADA** deverá substituir qualquer produto por outro novo e de primeiro uso, sempre que a soma dos períodos de paralisação do mesmo ultrapassar 05 (cinco) dias no prazo de 30 (trinta) dias corridos.

6.5. Caso haja necessidade de retirada de algum produto, para fins de reparo, a **CONTRATADA** deverá substituir por outro produto com características iguais ou superiores, sendo a instalação, configuração de responsabilidade da **CONTRATADA**. Esta substituição será em caráter definitivo se no prazo de 30 (trinta) dias a **CONTRATADA** não devolver o produto retirado em perfeitas condições de uso e ter sido notificada pela **CONTRATANTE**.

6.6. A **CONTRATADA** deverá disponibilizar para a **CONTRATANTE**, sem custo adicional, as respectivas atualizações de versões e "releases" de todos os produtos fornecidos, durante o período de garantia e deverá prestar a **CONTRATANTE** todo o suporte necessário para instalação e configuração das mesmas.

6.7. Durante o período de garantia de atualização técnica, a **CONTRATADA** deverá entregar as revisões dos manuais técnicos e/ou documentação dos softwares licenciados, sem ônus adicionais para a **CONTRATANTE**.

6.8. As novas versões do objeto contratado deverão ser disponibilizadas em até **05 (cinco) dias corridos**, a partir do lançamento oficial da versão.

6.9. A **CONTRATADA** garante à **CONTRATANTE** que os produtos licenciados para uso não infringem quaisquer patentes, direitos autorais ou trade-secrets.



**ESTADO DE MATO GROSSO**  
**SECRETARIA DE ESTADO DO MEIO AMBIENTE**  
**SECRETARIA ADJUNTA DE GESTÃO SISTÊMICA**  
**COORDENADORIA DE AQUISIÇÕES E CONTRATOS**  
**GERENCIA DE FORMALIZAÇÃO DE CONTRATOS**

**6.10.** Caso os produtos licenciados venham a ser objeto de ação judicial em que se discuta a infringência de patentes, direitos autorais ou trade-secrets, a **CONTRATADA** garante à **CONTRATANTE** que assumirá a direção defesa em juízo, responsabilizando-se pelos honorários advocatícios, custas processuais, bem como por todo e qualquer prejuízo.

**6.11. Produtividade de Referência**

**6.11.1.** Os profissionais que efetuarão a instalação, a configuração, implementação e o suporte técnico deverão ser certificados nos produtos adquiridos pela **CONTRATANTE**.

**6.11.2.** Os serviços serão executados na Seção de Informática da **CONTRATANTE** e será disponibilizado à **CONTRATADA**, local e meios materiais tais como: espaço físico, equipamentos, mobiliário, instalações e os meios de comunicação necessários ao desempenho e cumprimento dos serviços.

**6.12. Ordem de Serviço**

**6.12.1.** Será utilizado o procedimento de abertura de ordem de serviço para as comunicações formais.

**6.12.2.** A **CONTRATADA** deverá ofertar, dentro de seu Termo executivo, um modelo de ordem de serviço para aprovação pela comissão de recebimento, onde constem, no mínimo, os campos descritos abaixo, observando o previsto no Acordo de Nível de Serviço - ANS (item 7.13 deste Contrato).

- a) Descrição do chamado técnico;
- b) Data/hora da abertura do chamado técnico;
- c) Data/hora de chegada do(s) técnico(s) ao local do serviço;
- d) Registro do atendente;
- e) Registro do técnico solicitante;
- f) Número do ticket referente ao chamado;
- g) Registro do grau de severidade do chamado;
- h) Avaliação da qualidade do atendimento;
- i) Tempo total decorrido para o atendimento do chamado técnico (abertura do ticket à resolução do problema);



**ESTADO DE MATO GROSSO**  
**SECRETARIA DE ESTADO DO MEIO AMBIENTE**  
**SECRETARIA ADJUNTA DE GESTÃO SISTÊMICA**  
**COORDENADORIA DE AQUISIÇÕES E CONTRATOS**  
**GERENCIA DE FORMALIZAÇÃO DE CONTRATOS**

j) Tempo total decorrido para a resolução do problema (chegado do técnico ao local do atendimento à resolução do problema);

k) Relatório descritivo do serviço realizado; e

l) Aceite do serviço.

**6.12.3.** As aberturas das ordens de serviço se darão via 0800, telefone local, site e/ou e-mail específico, devendo estas informações de contato constar no Termo executivo da **CONTRATADA**.

**6.12.4.** Os atendimentos para aberturas das ordens de serviço deverão estar disponíveis 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, 365 (trezentos e sessenta e cinco) dias por ano.

**6.13. Acordo de Níveis de Serviço**

- Procedimentos e critérios de mensuração:

<b>Índice Nº 01 - Prazo de atendimento para demandas de Ordens de Serviço (OS) on-site</b>	
<b>Item</b>	<b>Descrição</b>
Finalidade	Garantir um atendimento célere e eficiente às demandas de suporte técnico on-site do COLOG e Diretorias Subordinadas, solicitadas por meio de Ordem de Serviço.
Meta a cumprir	Atender as demandas solicitadas por meio de Ordem de Serviço – OS, nos prazos estabelecidos neste índice com a troca de componentes e peças, caso necessário.
Método de medição	Cronometragem de tempo que se inicia após o recebimento da confirmação da solicitação da OS e a devida identificação (ticket de abertura), enviado por e-mail e/ou telefone à Contratante.
Forma de acompanhamento	Acompanhamento presencial do fiscal do contrato ou representante técnico por ele indicado durante a execução da OS até o seu encerramento.
Periodicidade	Mensal
Mecanismo de Cálculo do tempo de execução da OS	Somatório do número de horas de efetivo serviço - chegada do técnico da CONTRATADA ao local do atendimento até o final da execução da OS.
Tempo de restabelecimento do problema relatado na abertura da OS.	Após a chegada do técnico da CONTRATADA ao local do atendimento: - Até 02 (duas) horas para grau de severidade alto: e - Até 04 (quatro) horas para grau de severidade baixo.
Tempo esperado de atendimento para situações não críticas (grau de severidade baixo) - TASNC	Até 02 (duas) horas contadas a partir do início da medição até a chegada do técnico ao local de atendimento.



**ESTADO DE MATO GROSSO**  
**SECRETARIA DE ESTADO DO MEIO AMBIENTE**  
**SECRETARIA ADJUNTA DE GESTÃO SISTÊMICA**  
**COORDENADORIA DE AQUISIÇÕES E CONTRATOS**  
**GERENCIA DE FORMALIZAÇÃO DE CONTRATOS**

Tempo esperado de atendimento para situações críticas (grau de severidade alto) - TASC	Até 01 (uma) hora contada a partir do início da medição até a chegada do técnico ao local de atendimento.
Faixas de ajuste no pagamento - FAP	FAP01 - TASNC e TASC cumpridos dentro do estipulado neste índice, pagamento de 100% do valor da OS. FAP02 - TASC com atraso de 30 (trinta) minutos a 01 (uma) hora do estipulado neste índice, pagamento de 80% do valor da OS. FAP03 - TASNC com atraso de 30 (trinta) minutos a 01 (uma) hora do estipulado neste índice, pagamento de 90% do valor da OS. FAP04 - TASNC ou TASC com atraso superior a 60 (sessenta) minutos do estipulado neste índice, pagamento de 70% do valor da OS.
Sanções	Ocorrências de 02 eventos FAP02 por mês, multa de 30% sobre o valor total mensal contabilizado. Ocorrências de 02 eventos FAP03 por mês, multa de 20% sobre o valor total mensal contabilizado. Ocorrências de 02 eventos FAP04 por mês, multa de 40% sobre o valor total mensal contabilizado. Ocorrências de mais de 02 eventos FAPs quaisquer por mês, advertência na forma da lei. No caso de reincidência do parágrafo anterior, rescisão contratual, em conformidade com os procedimentos legais vigentes no COLOG.
Observações	- Às sanções aplicadas, se somarão os ajustes de pagamento (cumulativamente); - Os atrasos deverão ser informados no relatório descritivo do serviço realizado na OS.

**7. CLÁUSULA SÉTIMA – DAS OBRIGAÇÕES DA CONTRATANTE**

**7.1.** Emitir ORDEM DE FORNECIMENTO/SERVIÇO, conforme definido na cláusula sexta deste contrato, estabelecendo dia, hora, quantidade, local e demais informações que achar pertinentes para o bom cumprimento do objeto.

**7.2.** Receber os produtos adjudicados, nos termos, prazos, qualidade e condições estabelecidas neste contrato, no edital de **Pregão Eletrônico n.º 033/2013 – COLOG** e anexos, bem como, na **Ata de Registro de Preços n.º 00001/2013 do Exército Brasileiro/Ministério da Defesa**.



ESTADO DE MATO GROSSO  
SECRETARIA DE ESTADO DO MEIO AMBIENTE  
SECRETARIA ADJUNTA DE GESTÃO SISTÊMICA  
COORDENADORIA DE AQUISIÇÕES E CONTRATOS  
GERENCIA DE FORMALIZAÇÃO DE CONTRATOS

7.3. Proporcionar todas as facilidades indispensáveis para que o fornecedor possa cumprir suas obrigações dentro das normas e a boa execução das obrigações contratuais, inclusive permitindo o acesso de empregados, prepostos ou representantes da **CONTRATADA** em suas dependências;

7.4. Rejeitar, no todo ou em parte, os bens entregues em desacordo com as obrigações assumidas;

7.5. Acompanhar e fiscalizar a execução do objeto contratual, por meio do Fiscal do Contrato, nomeado mediante portaria publicada no Diário Oficial para exercer a fiscalização, o qual registrará em relatório as deficiências verificadas durante a execução do contrato, encaminhando cópias à **CONTRATADA** para a imediata correção das irregularidades apontadas, sem prejuízo da aplicação das penalidades previstas no Edital e neste contrato.

7.6. Comunicar formalmente qualquer anormalidade ocorrida na execução dos serviços pela **CONTRATADA**.

7.7. Informar a **CONTRATADA** de atos que possam interferir direta ou indiretamente nos serviços prestados.

7.8. Notificar a **CONTRATADA**, sempre que se fizer necessário, de qualquer irregularidade encontrada durante a execução do objeto contratual, para correção e/ou substituição nos termos deste contrato.

7.9. Estabelecer normas e procedimentos de acesso às suas instalações para a execução de serviços.

7.10. Avaliar todos os serviços prestados pela **CONTRATADA**.

7.11. Responsabilizar-se pelos pagamentos dos serviços prestados pela **CONTRATADA**, através de crédito em conta corrente mantida pela **CONTRATADA**, mediante a apresentação de Nota Fiscal/Fatura discriminativa.



**ESTADO DE MATO GROSSO**  
**SECRETARIA DE ESTADO DO MEIO AMBIENTE**  
**SECRETARIA ADJUNTA DE GESTÃO SISTÊMICA**  
**COORDENADORIA DE AQUISIÇÕES E CONTRATOS**  
**GERENCIA DE FORMALIZAÇÃO DE CONTRATOS**

**7.12.** Para os serviços de suporte técnico, a **CONTRATANTE** permitirá o acesso dos técnicos habilitados e identificados da **CONTRATADA** às instalações onde se encontrarem os equipamentos. Esses técnicos ficarão sujeitos a todas as normas internas de segurança da **CONTRATANTE**, inclusive àquelas referentes à identificação, trânsito e permanência em suas dependências.

**7.13.** Caso se interrompa a prestação dos serviços contratados, a área de Suporte deverá ter um plano de ação emergencial, de modo a amenizar os problemas surgidos. Este plano deverá ser elaborado juntamente com a equipe da **CONTRATADA**, devendo abordar em seu conteúdo procedimentos básicos para a execução dos serviços.

**8. CLÁUSULA OITAVA - DO PAGAMENTO**

**8.1.** O pagamento será realizado em até **30 (trinta) dias** após o adimplemento, aceitação e apropriação da solução de segurança entregue pela **CONTRATADA**, conforme subcláusula 2.2, mediante o recebimento da Nota fiscal e, após o atesto pelo fiscal do contrato e/ou responsáveis pelo recebimento, o qual deverá obedecer aos termos do Decreto nº 4.752, de 06 de agosto de 2002 c/c o Decreto nº 4.747, de 22 de junho de 1994, bem como na conformidade Decreto Estadual nº 8.199/2006.

**8.2.** O pagamento será efetivado por meio de Nota de Ordem Bancária, em nome da **CONTRATADA**, de acordo com a INSTRUÇÃO NORMATIVA Nº 001/2007-SAGP/SEFAZ, publicada no Diário Oficial do Estado em 25.05.2007;

**8.3.** A **CONTRATADA** indicará no corpo da Nota Fiscal o número e nome do banco, agência e número da conta onde deverá ser feito o pagamento, via ordem bancária, por intermédio do Banco do Brasil, para o banco discriminado.

**8.5.** A Nota Fiscal deverá estar em nome de ESTADO DE MATO GROSSO, com o CNPJ nº. 03.507.415/0023-50 e com o seguinte endereço: Rua C esquina com a Rua F, Centro Político Administrativo, Cuiabá-MT, CEP: 78.050-970.

**8.6.** Havendo erro na nota fiscal que impeça o pagamento da despesa, aquela será devolvida à **CONTRATADA** e o pagamento ficará pendente até que a mesma



**ESTADO DE MATO GROSSO**  
**SECRETARIA DE ESTADO DO MEIO AMBIENTE**  
**SECRETARIA ADJUNTA DE GESTÃO SISTÊMICA**  
**COORDENADORIA DE AQUISIÇÕES E CONTRATOS**  
**GERENCIA DE FORMALIZAÇÃO DE CONTRATOS**

providencie as medidas saneadoras. Nesta hipótese, o prazo para o pagamento iniciar-se-á após a regularização da situação ou reapresentação do documento fiscal, não acarretando qualquer ônus para a **CONTRATANTE**.

**8.7.** Nenhum pagamento deverá ser efetuado à **CONTRATADA**, enquanto pendente de liquidação qualquer obrigação. Esse fato não será gerador de direito a reajustamento de preços ou a atualização monetária.

**8.8.** Junto com a Nota Fiscal a **CONTRATADA** deverá obrigatoriamente apresentar Certidão Negativa de Débito dos Tributos Federais, Estaduais e Municipais, Certidão Negativa de Débito do FGTS e INSS, sem as quais fica impossibilitada a efetivação da liquidação do pagamento.

**8.9.** As comprovações de regularidade exigidas no subitem acima poderão ser substituídas pela regularidade junto ao Cadastro Geral de Fornecedores do Estado de Mato Grosso, conforme o caso.

**8.10.** As despesas bancárias decorrentes de transferência de valores para outras praças serão de responsabilidade da **CONTRATADA**.

**8.11.** Não haverá, sob hipótese alguma, pagamento antecipado.

**8.12.** O pagamento efetuado à **CONTRATADA** não a isentará de suas responsabilidades vinculadas ao fornecimento, especialmente aquelas relacionadas com a qualidade e garantia.

**8.13.** A partir de 1º de dezembro de 2010, as operações de vendas destinadas à Órgão Público da Administração Federal, Estadual e Municipal, deverão ser acobertadas por Nota Fiscal Eletrônica, conforme Protocolo ICMS42/2009, recepcionado pelo Artigo 198-A-5-2 do RICMS. Informações através do site [www.sefaz.mt.gov.br/nfe](http://www.sefaz.mt.gov.br/nfe).

## **9. CLÁUSULA NONA – DA DOTAÇÃO ORÇAMENTÁRIA**

**9.1.** As despesas decorrentes da execução do objeto deste contrato correrão por conta da seguinte dotação orçamentária:





ESTADO DE MATO GROSSO  
SECRETARIA DE ESTADO DO MEIO AMBIENTE  
SECRETARIA ADJUNTA DE GESTÃO SISTÊMICA  
COORDENADORIA DE AQUISIÇÕES E CONTRATOS  
GERENCIA DE FORMALIZAÇÃO DE CONTRATOS

Órgão/Unidade: 27101 - SECRETARIA DE ESTADO DO MEIO AMBIENTE
Projeto Atividade: 4318
Natureza de Despesa: 4490 5200/3390 3900
Fonte de Recurso: 309

9.2. As despesas decorrentes do objeto desta contratação, no exercício seguinte, correrão à conta dos recursos específicos consignados no orçamento do órgão.

#### 10. CLÁUSULA DÉCIMA - DA VIGÊNCIA

10.1. A vigência do presente contrato será de **12 (doze) meses**, contados após a publicação de seu extrato no Diário Oficial do Estado de Mato Grosso.

10.1.1. Este contrato poderá ser prorrogado, por iguais e sucessivos períodos, até o limite de **36 (trinta e seis) meses**, para fins de cobertura do serviço de suporte/assistência técnica, vinculados à garantia do objeto, sem desembolso financeiro.

#### 11. CLÁUSULA DÉCIMA PRIMEIRA - DA RESCISÃO

11.1. A rescisão regula-se pelo disposto nos artigos 77 a 80 da Lei nº. 8.666/93, no que couber.

11.1.1. No caso de rescisão administrativa, a **CONTRATANTE** poderá executar a garantia de execução para ressarcimento dos valores de multa e indenização a ela devidos e reter os créditos decorrentes deste contrato até o limite dos prejuízos causados à **CONTRATANTE**, sem prejuízo das sanções da lei.

#### 12. CLÁUSULA DÉCIMA SEGUNDA - DAS SANÇÕES ADMINISTRATIVAS

12.1. O não cumprimento das obrigações contratuais sujeitará a **CONTRATADA**, garantida prévia defesa, às seguintes sanções:



**ESTADO DE MATO GROSSO**  
**SECRETARIA DE ESTADO DO MEIO AMBIENTE**  
**SECRETARIA ADJUNTA DE GESTÃO SISTÊMICA**  
**COORDENADORIA DE AQUISIÇÕES E CONTRATOS**  
**GERENCIA DE FORMALIZAÇÃO DE CONTRATOS**

12.1.1. advertência;

12.1.2. multa de mora de 0,1 % (um décimo por cento) calculada sobre o valor do contrato, por até 90 (noventa) dias de atraso injustificado na execução dos serviços (cobrada por dia de atraso);

12.1.3. multa de mora de 0,2 % (dois décimos por cento) calculada sobre o valor do contrato de 90 (noventa) a 180 (cento e oitenta) dias de atraso injustificado na execução dos serviços (cobrada por dia de atraso);

12.1.4. multa de mora 0,3 % ( três décimos por cento ) calculada sobre o valor do contrato, acima de 180 (cento e oitenta) dias , por dias de atraso injustificado na execução dos serviços (cobrada por dia de atraso);

12.1.5. multa de 0,1 % (um décimo por cento) sobre o valor do contrato por dia de atraso injustificado pela reapresentação do material rejeitado, depois de esgotado o prazo fixado para substituição, correção ou reparação; e

12.1.6. multa de 30% (trinta por cento) sobre o valor do contrato, em caso de rescisão causada por ação ou omissão injustificada da contratada.

12.2. Ficará impedida de licitar e contratar com o Estado e descredenciada no Cadastro Geral de Fornecedores, pelo prazo de até 05 (cinco) anos, sem prejuízo das multas previstas neste contrato e demais cominações legais, a licitante que:

12.2.1. deixar de entregar documentação exigida neste contrato ou apresentar documentação falsa;

12.2.2. ensejar o retardamento da execução do objeto da licitação;

12.2.3. não mantiver a proposta;

12.2.4. falhar ou fraudar na execução do contrato;

12.2.5. comportar-se de modo inidôneo;

12.2.6. fizer declaração falsa; ou

12.2.7. cometer fraude fiscal.

12.3. As multas poderão ser aplicadas concomitantemente com as demais sanções, facultada a defesa prévia do interessado no prazo de 05 (cinco) dias úteis, contados a partir da data em que tomar ciência.



**ESTADO DE MATO GROSSO**  
**SECRETARIA DE ESTADO DO MEIO AMBIENTE**  
**SECRETARIA ADJUNTA DE GESTÃO SISTÊMICA**  
**COORDENADORIA DE AQUISIÇÕES E CONTRATOS**  
**GERENCIA DE FORMALIZAÇÃO DE CONTRATOS**

**12.4.** Para efeito de aplicação de multa, o valor do contrato será apurado deduzindo-se dele o valor das entregas realizadas dentro do prazo pactuado e aceitas pela **CONTRATANTE**.

**12.5.** A aplicação das sanções previstas neste contrato não exclui a possibilidade da responsabilidade civil da **CONTRATADA** por eventuais perdas e danos à Administração Pública.

**12.6.** A multa, aplicada após regular processo administrativo, será descontada da garantia do respectivo contratado.

**12.7.** Se a multa for de valor superior ao valor da garantia prestada, além da perda desta, responderá a **CONTRATADA** pela sua diferença, a qual será descontada dos pagamentos eventualmente devidos pela Administração ou ainda, quando for o caso, cobrada judicialmente.

**13. CLÁUSULA DÉCIMA TERCEIRA - DO DIREITO DE PETIÇÃO**

**13.1.** No tocante a recursos, representações e pedidos de reconsideração, deverá ser observado o disposto no art. 109 da Lei nº 8.666/93.

**14. CLÁUSULA DÉCIMA QUARTA - DA FISCALIZAÇÃO E ACOMPANHAMENTO**

**14.1.** Será designado pela **Coordenadoria de Tecnologia da Informação** da **CONTRATANTE**, um servidor qualificado ou uma comissão para exercer a fiscalização do contrato, que terá, dentre outras, a incumbência de solicitar à **CONTRATADA** o afastamento ou a substituição de profissional que considere ineficiente, incompetente, inconveniente ou desrespeitoso com pessoas da **CONTRATANTE** ou terceiros ligados ao objeto do contrato, obrigando-se a **CONTRATADA** a facilitar, de modo amplo e irrestrito, a ação do fiscal do contrato.

**PARÁGRAFO ÚNICO** - O exercício da fiscalização pela **CONTRATANTE** não excluirá nem reduzirá as responsabilidades de competência da **CONTRATADA**.



**ESTADO DE MATO GROSSO**  
**SECRETARIA DE ESTADO DO MEIO AMBIENTE**  
**SECRETARIA ADJUNTA DE GESTÃO SISTÊMICA**  
**COORDENADORIA DE AQUISIÇÕES E CONTRATOS**  
**GERENCIA DE FORMALIZAÇÃO DE CONTRATOS**

**14.2.** Serão previstas, a critério da **CONTRATANTE**, visitas técnicas às instalações da **CONTRATADA** onde se processar a execução dos serviços contratados.

**14.3.** A **CONTRATANTE** reserva-se ao direito de, sem que de qualquer forma restrinja a plenitude da responsabilidade da **CONTRATADA**, exercer a mais ampla e completa fiscalização sobre o objeto contratado, cabendo-lhe, entre outras providências de ordem técnica, conferir o serviço fornecido e atestar as notas fiscais, observado o que consta no Acordo de Nível de serviço - ANS.

**15. CLÁUSULA DÉCIMA QUINTA - DAS DISPOSIÇÕES GERAIS**

**15.1.** Este contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas previstas na Lei nº 8.666/93, respondendo elas pelas consequências de sua inexecução total ou parcial;

**15.2.** A **CONTRATADA** fica obrigada a aceitar nas mesmas condições contratuais, os acréscimos ou supressões, que, a critério da **CONTRATANTE**, se façam necessários, até o limite de 25% do valor global deste contrato;

**15.2.1.** As supressões poderão ultrapassar o limite acima estabelecido, havendo acordo entre as partes;

**15.3.** A **CONTRATANTE** poderá revogar este contrato, por razões de interesse público decorrente de fato superveniente, devidamente comprovado, pertinente e suficiente para justificar tal conduta, devendo anulá-lo por ilegalidade, de ofício ou por provocação de terceiros, mediante parecer escrito e devidamente fundamentado;

**15.3.1.** A declaração de nulidade deste contrato opera retroativamente, impedindo efeitos jurídicos que nele, ordinariamente, deverá produzir, além de desconstituir os que porventura já tenha produzido;



**ESTADO DE MATO GROSSO  
SECRETARIA DE ESTADO DO MEIO AMBIENTE  
SECRETARIA ADJUNTA DE GESTÃO SISTÊMICA  
COORDENADORIA DE AQUISIÇÕES E CONTRATOS  
GERENCIA DE FORMALIZAÇÃO DE CONTRATOS**

**15.3.2.** A nulidade não exonera a **CONTRATANTE** do dever de indenizar a **CONTRATADA** pelo que esta houver executado até a data em que ela for declarada e por outros prejuízos regularmente comprovados, contanto que não lhe seja imputável, promovendo a responsabilidade de quem lhe deu causa.

**16. CLÁUSULA DÉCIMA SEXTA - DO FORO**

**16.1.** Fica eleito o foro da cidade de Cuiabá, Estado de Mato Grosso, como competente para dirimir quaisquer dúvidas ou questões decorrentes da execução deste contrato.

E, por se acharem justas e contratadas, as partes assinam o presente instrumento na presença das testemunhas abaixo, em 02 (duas) vias de igual teor e forma, para que produza todos os efeitos legais.

Cuiabá, 28 de novembro de 2014.

\_\_\_\_\_  
**BENEDITO NERY GUARIM STROBEL**  
Secretário Adjunto de Gestão Sistêmica  
SEMA/MT

\_\_\_\_\_  
**GUSTAVO LIMA MIRANDA**  
Representante da Contratada

**TESTEMUNHAS:**

**KELLY ALMEIDA KORMANN**  
CPF: 823.964.001-00

**FERNANDA B. C. DE SOUZA CARVALHO**  
CPF: 973.078.581-34



**ESTADO DE MATO GROSSO**  
**SECRETARIA DE ESTADO DO MEIO AMBIENTE**  
**SECRETARIA ADJUNTA DE GESTÃO SISTÊMICA**  
**COORDENADORIA DE AQUISIÇÕES E CONTRATOS**  
**GERENCIA DE FORMALIZAÇÃO DE CONTRATOS**

**ANEXO I – ESPECIFICAÇÕES TÉCNICAS (DETALHAMENTO): Item 03 - Solução de IPS TIPO I**

Licenças de uso de software IPS, por um período de 36 (trinta e seis meses) conforme características listadas abaixo:

3.1 A solução deve ser fornecida em equipamento e deve possuir a seguinte configuração:

- Tráfego agregado: 200 MBPS (Megabits por segundo)
- Conexões concorrentes: 80.000
- DoS (Denial of Service) profiles: 120
- Virtual IDS/IPS: 64 por equipamento – 64 por interface
- Regras por ACL (Access Control List): 100
- Interfaces de monitoração gigabit ethernet: 8 unidades de cobre (10BASE-T/100BASE-TX/1000BASE-T)
- Interface dedicada de gerência: 1 unidade de cobre (10BASE-T/100BASE-TX/1000BASE-T)
- Interface dedicada de resposta: 1 unidade de cobre (10BASE-T/100BASE-TX)
- Interface dedicada de console: 1 Serial (RS-232C)

3.2 O equipamento deve ser baseado em appliance Box;

3.3 O equipamento deve ser baseado em SSD1 (Solid State Drive) sem HD (Hard Disc) com arquitetura ASIC2 (Application Specific Integrated Circuit) e FPGA3 (Field Programmable Gate Array), isto é, o equipamento deve ser desenvolvido, tanto software quanto hardware, para a funcionalidade única, exclusiva e especificamente de Network Intrusion Prevention;

3.4 O equipamento deve suportar integração com TACACS+ para autenticação de usuários e administradores;

3.5 O equipamento deve possuir LED (Light-Emitting Diode), no painel frontal, para fornecer informações sobre Health Status – fonte(s) de energia, sistema, ventilação e temperatura do ar de entrada – do equipamento e atividades das interfaces;

3.6 O equipamento não deve necessitar de reconfiguração de routers e/ou switches para sua instalação em InLine Mode;

3.7 O equipamento deve suportar tecnologia que permita uma inspeção inteligente baseada em análise estatística do fluxo de dados de rede, otimizando o processo de identificação e proteção contra ataques;

3.8 O equipamento deve suportar monitoração e proteção de segmentos de rede em modo transparente e operação na camada 2 (Layer-2) do modelo OSI (Open System Interconnection) – Bridge Mode. Isto é, as interfaces de monitoração e proteção não requerem endereço IP;

3.9 O equipamento deve suportar tanto configuração manual de velocidade e Duplex quanto configuração automática de auto-negociação baseada na especificação IEEE 802.3u das interfaces;

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

3.11 O equipamento deve suportar funcionamento como Firewall transparente, permitindo a criação de regras para filtros de acesso de camada 3;

3.12 O equipamento deve suportar configuração, manutenção e visualização de estado das interfaces de monitoração e proteção através de CLI (Command Line Interface – Interface de Linha de Comando);

3.13 O equipamento deve suportar as modalidades de instalação:

- SPAN Mode: monitoração e proteção de HUBS e/ou portas SPAN de switches, com o tráfego ativo de redes sendo espelhado para ele, permitindo monitorar ataques trafegando por estes espelhamentos e respondendo em tempo real, sendo altamente granulares as ações preventivas;

- TAP Mode: monitoração e proteção de comunicações de rede em ambas as direções em Full-Duplex, permitindo monitorar ataques trafegando por estas comunicações, mantendo o estado destas e respondendo em tempo real, sendo altamente granular as ações preventivas;

- InLine Mode: monitoração e proteção de segmentos de dados, com tráfego ativo de rede passando por ele, permitindo impedir ataques trafegando por estes segmentos e bloqueando-os em tempo real, sendo altamente granulares as ações preventivas;

3.14 O equipamento deve suportar criação, configuração e manutenção de Virtual IPS e Virtual Firewall através de VLAN Tagging 802.1Q ou bloco(s) de endereços (CIDR – Classless Inter-Domain Routing), assim como criação, configuração e manutenção de Port Clustering através do agrupamento de múltiplas interfaces físicas em uma única Virtual Interface;

3.15 O equipamento deve possuir Built-in Network TAP;



**ESTADO DE MATO GROSSO**  
**SECRETARIA DE ESTADO DO MEIO AMBIENTE**  
**SECRETARIA ADJUNTA DE GESTÃO SISTÊMICA**  
**COORDENADORIA DE AQUISIÇÕES E CONTRATOS**  
**GERENCIA DE FORMALIZAÇÃO DE CONTRATOS**

- 3.16 O equipamento deve suportar monitoração, proteção, decodificação, análise e bloqueio de tráfego de aplicações Instant Messenger e P2P (Peer-to-Peer), tais como: AOL Instant Messenger, AOL Instant Messenger Express, Ares, Azureus, Bearshare, Bittorrent, Blubster, DirectConnect, eDonkey, eMule, Enpy, ICQ, ICQ2Go, FileNara, Gnucleus, Gnutella, Grokster, Groove, JAP Anonymizer, Kazaa, Limewire, Morpheus, MSN Messenger, Mutella, MyNapster, Mxie, OpenLITO, Overnet, Phex, Piolet, RockItNet, Shareaza, Skype, SoulSeek, Swapper, Xolox, WinMX, Yahoo! Messenger, etc;
- 3.17 O equipamento deve suportar montagem em Rack 19";
- 3.18 O equipamento deve suportar redundância de fonte de energia;
- 3.19 O equipamento deve suportar detecção da falha no equipamento, deve suportar detecção de link;
- 3.20 O equipamento deve suportar Corrente Alternada ou Alternada (AC – Alternating Current) ou Corrente Contínua ou Galvânica (DC – Direct Current);
- 3.21 O equipamento deve suportar Fail-close e Fail-open (Layer-2 Passthru e Hardware Bypass);
- 3.22 O equipamento deve suportar HA (High Availability – Alta-disponibilidade) ativo-passivo;
- 3.23 O equipamento deve suportar HA (High Availability – Alta-disponibilidade) ativo-ativo – utilizando-se apenas de uma (01) a duas (02) interfaces por equipamento do HA Pair;
- 3.24 O equipamento deve suportar HA (High Availability – Alta-disponibilidade) Statefull Failover;
- 3.25 O equipamento deve suportar ambiente com balanceamento de carga através de um ou dois equipamentos;
- 3.26 Deve suportar ajuste de gestão de tráfego granular (On/Off) por interfaces físicas do equipamento;
- 3.27 Deve suportar Rate Limiting:
- Otimização de quantidade de tráfego permitido através de uma interface de rede, baseando-se em limitações de banda impostas à protocolos de rede;
  - Marcação do tráfego (QoS – Quality of Service) a serem tratados por routers, switches e/ou demais dispositivos da infraestrutura de rede.
- 3.28 Deve suportar VLAN Tagging 802.1p (CoS – Class Of Service);
- 3.29 Deve suportar DiffServ (Differentiated Services);
- 3.30 Deve suportar a utilização de dois algoritmos comumente usados para Traffic Shaping ou Rate Limiting:
- Leaky Bucket Algorithm;
  - Token Bucket Algorithm;
- 3.31 Deve suportar as seguintes quantidades de filas:
- Rate Limiting: Até seis (06) filas para interfaces 100BASE-TX e oito (08) filas para interfaces 1000BASE-T, 1000BASE-SX, 1000BASE-LX, 10GBASE-SR e 10GBASE-LR;
  - VLAN Tagging 802.1p (CoS – Class Of Service): Até oito (08) filas para interfaces 100BASE-TX, 1000BASE-T, 1000BASE-SX, 1000BASE-LX, 10GBASE-SR e 10GBASE-LR;
  - DiffServ (Differentiated Services): Até sessenta e quatro (64) filas para interfaces 100BASE-TX, 1000BASE-T, 1000BASE-SX, 1000BASE-LX, 10GBASE-SR e 10GBASE-LR;
- 3.32 Deve suportar roteamento e tráfego assimétrico;
- 3.33 Deve suportar monitoração, proteção, decodificação, análise e bloqueio de ataques através de:
- Segmentos com VLAN Tagging 802.1Q. 2. Segmentos com Stacked VLAN;
  - Segmentos com Jumbo Frames. 4. Segmentos com QnQ (Double VLAN Tagging). 5. Segmentos com ECLB (EtherChannel Load Balancing). 3. Segmentos com VLAN Bridging em STP (Spanning Tree Protocol);
  - Segmentos com MPLS (Multi Protocol Label Switching);
  - Segmentos com GRE (Generic Routing Encapsulation);
  - Segmentos com GPRS (General Packet Radio Service) Tunneling Protocol;
- 3.34 Deve suportar monitoração, proteção, decodificação, análise e bloqueio de ataques através de:
- Tráfego com IPv6 nativo com túneis: 4in4, 4in6, 6in4 e 6in6.
  - Tráfego com criptografia SSL (Secure Sockets Layer) 10 com certificados PKCS12;
- 3.35 Deve suportar assinaturas para ataques de vulnerabilidades DoS (Denial of Service), tais como:
- Logic Attacks: boink, bonk, jolt, land, latierra, nestea, newtear, pimp, ping-of-death, reset-tcp, rose, rst\_flip, smurf, snork, teardrop, winnuke, etc;



**ESTADO DE MATO GROSSO**  
**SECRETARIA DE ESTADO DO MEIO AMBIENTE**  
**SECRETARIA ADJUNTA DE GESTÃO SISTÊMICA**  
**COORDENADORIA DE AQUISIÇÕES E CONTRATOS**  
**GERENCIA DE FORMALIZAÇÃO DE CONTRATOS**

- Bandwidth Attacks: ICMP echo request Flood, TCP data segment Flood, TCP SYN/RST Flood, IP fragment Flood, etc;
- Protocol Attacks: SYN Flood, Smurf, Fraggle, etc;
- 3.36 Deve suportar assinaturas para ferramentas de ataques DDoS (Distributed Denial of Service), tais como: Trinoo, Shaft, Stacheldraht, Trinity, TFN, TFN2K, MStream, etc;
- 3.37 Deve suportar assinaturas baseadas em thresholds;
- 3.38 Deve suportar DoS/DDoS Profiles<sup>11</sup> e Self-Learning, possibilitando-se:
  - Gerência de perfis de DoS múltiplos;
  - Gerência de perfis de tráfegos de curto e médio prazo, através da importância quantitativa na mudança do tráfego; - Monitoração, proteção, decodificação, análise e bloqueio de anomalias categóricas ou desequilíbrio do tráfego ICMP ECHO Anomalies - type:8/code:0 e type:0/code:0 e TCP Control Segment Anomalies (SYN, SYN-ACK, FIN and RST);
- 3.39 A solução deve possuir recursos de monitoração, proteção, decodificação, análise e bloqueio de ataques DoS (Denial of Service) e DDos (Distributed Denial of Service) através de anomalias de volume de tráfego:
  - IP fragment
  - ICMP ECHO (type:8/code:0 e type:0/code:0)
  - Todos os outros ICMP
  - UDP
  - TCP SYN e FIN
  - TCP RST
  - Non-TCP/UDP/ICMP
  - Out-of-Window TCP data segment
  - Out-of-Context TCP data segment
- 3.40 A solução deve possuir recursos de monitoração, proteção, decodificação, análise e bloqueio de ataques:
  - TCP SYN e ACK Flood;
  - UDP Flood;
  - ICMP Flood;
- 3.41 O equipamento deve suportar assinaturas baseadas em ataques direcionados à DNS;
- 3.42 O equipamento deve suportar monitoração, proteção, decodificação e análise stateful inspection, mantendo o estado das sessões monitoradas, podendo optar-se também por monitoração e proteção stateless inspection;
- 3.43 O equipamento deve suportar monitoração, proteção, decodificação e análise de ataques independente do sistema operacional alvo;
- 3.44 O equipamento deve suportar identificação passiva dos sistemas operacionais (Passive OS Fingerprint) dos sistemas monitorados e protegidos;
- 3.45 O equipamento deve suportar monitoração, proteção, decodificação e análise do tráfego na direção servidor-cliente, para detecção e bloqueio de exploits originados em servidores e direcionados aos clientes (drive-by attacks);
- 3.46 O equipamento deve suportar monitoração, proteção, decodificação e análise para ameaças APT12 (Advanced Persistent Threat – Ameaças Avançadas e Persistentes);
- 3.47 O equipamento deve suportar monitoração, proteção, decodificação e análise do tráfego em redes de automação SCADA (Supervisory Control And Data Acquisition);
- 3.48 Deve suportar os seguintes ataques:
  - Reconnaissance: Host Sweep, Port Scan, Brute Force, Service Sweep, OS Fingerprint;
  - Exploits: Protocol Violation, Buffer Overflow, Shellcode Execution, Remote Access, Privileged Access, Probe, DoS (1.Logic Attacks: boink, bonk, jolt, land, latierra, nestea, newtear, pimp, ping-of-death, reset-tcp, rose, rst\_flip, smurf, snork, teardrop, winnuke, etc;
  - Bandwidth Attacks: ICMP echo request Flood, TCP data segment Flood, TCP SYN/RST Flood, IP fragment Flood, etc;
  - Protocol Attacks: SYN Flood, Smurf, Fraggle, etc., Evasion Attempt, Arbitrary Command Execution, Code/Script Execution, Bot (Agobot, Al3na Monster, Floodnet, etc.), Trojan (BackOrifice 2000; Dagger; Infector 1.7, etc.), DDos Agent Activity, Backdoor, Worms (Slapper e variações; Slammer e variações; Blaster e variações; Sasser e variações; Zotob e variações; Confinker e variações; etc.), Virus, Read Exposure, Write Exposure;





**ESTADO DE MATO GROSSO**  
**SECRETARIA DE ESTADO DO MEIO AMBIENTE**  
**SECRETARIA ADJUNTA DE GESTÃO SISTÊMICA**  
**COORDENADORIA DE AQUISIÇÕES E CONTRATOS**  
**GERENCIA DE FORMALIZAÇÃO DE CONTRATOS**

- Volume DoS: Statistical Deviation, Over Threshold;
- Policy Violations: Audit, Restricted Access, Restricted Application, Unauthorized IP, Sensitive Content, Covert;
- 3.49 A solução deve possuir IP Defragmentation – defragmentação dos pacotes IP fragmentados e/ou sobrepostos;
- 3.50 A solução deve possuir TCP Stream Reassembly – remontagem dos pacotes TCP fragmentados e/ou sobrepostos e dos fluxos (Flows) TCP;
- 3.51 A solução deve possuir Detailed Protocol Analysis – análise e decodificação de 200 protocolos de rede (Layer-2 to Layer-7 – camada 2 à camada 7), permitindo a monitoração, proteção, decodificação e análise de ataques desconhecidos e/ou múltiplas variantes de um ataque sem atualização de assinaturas. Estão inclusos, entre outros, os protocolos:
- Application Layer: BGP, CIFS, DHCP, DNS, FTP, GTP, H.225, H.323, HTTP, IMAP, IRC, Kerberos, LDP, MS-RPC, NFS, NNTP, NTP, NetBIOS, NamedPipes, POP, RIP, DCE-RPC, MS-RPC, SUN-RPC, RTP, SIP, SMTP, SNMP, SSH, SSL, SSRP, TELNET, TDS, etc.
- Transport Layer: TCP, UDP, OSPF, etc.
- Internet Layer: IPv4, IPv6, ICMP, ICMPv6, IGMP, etc.
- 3.52 A solução deve possuir Advanced Evasion Protection – proteção e resistência à técnicas de evasão (False-negatives) e/ou ataques direcionados ao equipamento. Entre estas proteções estão inclusos:
- Fragmentação de pacotes nos protocolos de camada 7 (Layer-7): DCE-RPC, MS-RPC, SUN-RPC, NetBIOS, NamedPipes, TDS, etc;
- Códigos Polimórficos (Polymorphic Shellcode): alpha2, “finstenv / mov”, Countdown, “jmp / call additive”, ShikataGaNaI, “call+4 dword / xor”, etc;
- SNMP Flood;
- Sobreposição de pacotes (Packet Overlapping);
- RPC Record Marking e RPC Encryption;
- HTTP Obfuscation: Hex & Double-Hex Encoding, Base-64 Encoding, Unicode/UTF-8 Encoding, MS IIS %u Encoding, Self-referential Directory, Directory Transversal, etc;
- Ferramentas de evasão: whisker, libwhisker, nikto, fragroute, fragrouter, etc;
- Stealth Port Scan: Nmap, Hping2, Hping3, etc. 9. DoS (Denial of Service) através de False-positive Flood e conexões stateless: Snot, Stick, IDS-Wakeup, NNG, etc;
- 3.53 A solução deve possuir Protocol Tunneling - análise e decodificação de protocolos encapsulados em tráfegos:
- VLAN Tagging 802.1Q e QnQ (Double VLAN Tagging);
- Jumbo Frames. 3. ECLB (EtherChannel Load Balancing) e VLAN Bridging em STP (Spanning Tree Protocol);
- MPLS (Multi Protocol Label Switching);
- GRE (Generic Routing Encapsulation);
- GPRS (General Packet Radio Service) Tunneling Protocol;
- IPv6 nativo e túneis: 4in4, 4in6, 6in4 e 6in6. 8. SSL (Secure Sockets Layer)<sup>15</sup> com certificados PKCS12;
- 3.54 A solução deve possuir Heuristics Analysis – detecção e análise baseada em procedimentos heurísticos, utilizando-se dados evidenciados, lógica computacional, algoritmos matemáticos e algoritmos seletivos para avaliar e detectar novos ataques com alto desempenho e precisão. Estão inclusos, entre outros, os algoritmos:
- Shellcode Heuristics: algoritmos proprietários para detecção de ataques de Buffer Overflow em plataformas IA-32 (x86), IA-64, PPC, MIPS, SPARC, RISC.
- Peer-to-Peer (P2P) Heuristic: algoritmos proprietários para detecção de conexões P2P evasivas, transferências de arquivos criptografadas e com técnicas de “Obfuscated Binary”.
- 3.55 A solução deve possuir Protocol Normalization – verificação de conformidade RFC e/ou especificações dos protocolos, tais como: RFC 1034, RFC 1035, RFC 1050, RFC 1057, RFC 1112, RFC 114, RFC 1194, RFC 1196, RFC 1288, RFC 1329, RFC 1349, RFC 1413, RFC 1459, RFC 1531, RFC 1579, RFC 1831, RFC 1883, RFC 1885, RFC 1945, RFC 2068, RFC 2069, RFC 2225, RFC 2228, RFC 2236, RFC 2333, RFC 2407, RFC 2408, RFC 2409, RFC 2428, RFC 2460, RFC 2463, RFC 2474, RFC 2616, RFC 2617, RFC 2640, RFC 265, RFC 2734, RFC 2780, RFC 2810, RFC 2811, RFC 2812, RFC 2813, RFC 2817, RFC 2834, RFC 2835, RFC 3376, RFC 354, RFC 3659, RFC 4294, RFC 4306, RFC 4338, RFC 4380, RFC 4443, RFC 4884, RFC 4890, RFC 5095, RFC 5282, RFC 542, RFC 5494, RFC 5531, RFC 742, RFC 760, RFC 765, RFC 768, RFC 777, RFC 791, RFC



**ESTADO DE MATO GROSSO**  
**SECRETARIA DE ESTADO DO MEIO AMBIENTE**  
**SECRETARIA ADJUNTA DE GESTÃO SISTÊMICA**  
**COORDENADORIA DE AQUISIÇÕES E CONTRATOS**  
**GERENCIA DE FORMALIZAÇÃO DE CONTRATOS**

792, RFC 793, RFC 826, RFC 912, RFC 931, RFC 950, RFC 951, RFC 959, ETSI GSM ES 09.60, 3GPP TS 29.060, 3GPP TS 32.295, 3GPP TS 29.274, ITU-T H.225.0, ITU-T H.323, IEEE 802.1Q, MS-TDS 2.0, MS-SQLR 1.2, etc;

3.56 A solução deve possuir Pattern Matching Signatures – assinaturas por compração de padrões de dados (Pattern Matching);

3.57 A solução deve possuir OpenSource Signatures – assinaturas baseadas em padrão aberto – também conhecidas como assinaturas baseadas em OpenSource ou SNORT – permitindo tanto a criação de novas assinaturas quanto importá-las e havendo uma comparação da identificação CVE (Common Vulnerability Exposure) para evitar duplicidade de eventos;

3.58 A solução deve possuir Vulnerability Based Signatures – assinaturas baseadas na vulnerabilidade, permitindo a monitoração, proteção, decodificação e análise de ataques desconhecidos e/ou múltiplas variantes de um ataque sem atualização de assinaturas;

3.59 A solução deve possuir Custom Attacks Signatures – assinaturas criadas pelo administrador, possibilitando a utilização de REGEX (Regular Expression) ou processo automático de criação de assinatura à partir de um tráfego capturado na rede;

3.60 A solução deve possuir Statisticas Anomaly – detecção e análise baseada em estatísticas por tráfego de protocolos;

3.61 A solução deve possuir Protocol Anomaly – validação de campos de cabeçalho inválidos, pacotes mal-formatados, pacotes ilegais e conformidade RFC e/ou especificações dos protocolos, tais como: RFC 1034, RFC 1035, RFC 1050, RFC 1057, RFC 1112, RFC 114, RFC 1194, RFC 1196, RFC 1288, RFC 1329, RFC 1349, RFC 1413, RFC 1459, RFC 1531, RFC 1579, RFC 1831, RFC 1883, RFC 1885, RFC 1945, RFC 2068, RFC 2069, RFC 2225, RFC 2228, RFC 2236, RFC 2333, RFC 2407, RFC 2408, RFC 2409, RFC 2428, RFC 2460, RFC 2463, RFC 2474, RFC 2616, RFC 2617, RFC 2640, RFC 265, RFC 2734, RFC 2780, RFC 2810, RFC 2811, RFC 2812, RFC 2813, RFC 2817, RFC 2834, RFC 2835, RFC 3376, RFC 354, RFC 3659, RFC 4294, RFC 4306, RFC 4338, RFC 4380, RFC 4443, RFC 4884, RFC 4890, RFC 5095, RFC 5282, RFC 542, RFC 5494, RFC 5531, RFC 742, RFC 760, RFC 765, RFC 768, RFC 777, RFC 791, RFC 792, RFC 793, RFC 826, RFC 912, RFC 931, RFC 950, RFC 951, RFC 959, ETSI GSM ES 09.60, 3GPP TS 29.060, 3GPP TS 32.295, 3GPP TS 29.274, ITU-T H.225.0, ITU-T H.323, IEEE 802.1Q, MS-TDS 2.0, MS-SQLR 1.2, etc;

3.62 A solução deve possuir Application Anomaly – validação de campos e conformidade de especificação dos protocolos Layer-7 (camada 7). Estão inclusos, entre outros, os protocolos:

- Application Layer: BGP, CIFS, DHCP, DNS, FTP, GTP, H.225, H.323, HTTP, IMAP, IRC, Kerberos, LDP, MS-RPC, NFS, NNTP, NTP, NetBIOS, NamedPipes, POP, RIP, DCE-RPC, MS-RPC, SUN-RPC, RTP, SIP, SMTP, SNMP, SSH, SSL, SSRP, TELNET, TDS, etc;

- Transport Layer: TCP, UDP, OSPF, etc;

- Internet Layer: IPv4, IPv6, ICMP, ICMPv6, IGMP, etc;

3.63 A solução deve possuir proteção em Cloud Computing, ou seja, monitoração, proteção, decodificação e análise stateless de ataques desconhecidos e/ou múltiplas variantes de um ataque através de utilização de tecnologia em nuvem (Cloud Computing), sem atualização de assinaturas;

3.64 A solução deve possuir recurso de monitoração, proteção, decodificação e análise comportamental baseada em tecnologia em nuvem (Cloud Computing) para identificar códigos maliciosos originados em servidores e direcionados aos clientes (drive-by attacks);

3.65 A solução deve possuir recurso de monitoração, proteção, decodificação e análise baseada em reputação por pontuação (Score Reputation) de identificadores, tais como: endereço IP, URL (Uniform Resource Locator) e domínio;

3.66 A console de gerenciamento da solução deve suportar instalação em ambientes virtualizados com VMware ESX 3.x;

3.67 A console de gerenciamento da solução deve suportar instalação em equipamento baseado em modelo Appliance Box, dotado de processamento e memória compatíveis;

3.68 A console de gerenciamento da solução deve suportar sincronismo de horário através de NTP (Network Time Protocol);

3.69 A solução deve suportar instalação em HA (High Availability – Alta-disponibilidade) ativo-passivo;

3.70 A solução deve suportar atualização:

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

- Offline: automática e/ou manual de conteúdo de segurança e produto

3.71 A solução deve suportar autenticação de usuários e administradores através:

- Autenticação local: usuários e administradores cadastrados na gerência;



**ESTADO DE MATO GROSSO**  
**SECRETARIA DE ESTADO DO MEIO AMBIENTE**  
**SECRETARIA ADJUNTA DE GESTÃO SISTÊMICA**  
**COORDENADORIA DE AQUISIÇÕES E CONTRATOS**  
**GERENCIA DE FORMALIZAÇÃO DE CONTRATOS**

- Autenticação LDAP: usuários e administradores importados/integrados com o Windows AD (Active Directory), permitindo: SSL (Secure Sockets Layer) e Non-SSL (Secure Sockets Layer);
- Autenticação RADIUS: usuários e administradores importados/integrados com servidor RADIUS, permitindo: PAP (Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol) e EAP-MD5 (Extensible Authentication Protocol-MD5);
- 3.72 A solução deve suportar atribuição de perfis para usuário e administradores, tais como:
  - Administrador IPS (Intrusion Prevention System);
  - Gerente de contas de portal de segurança;
  - Operador NOC (Network Operation Center);
  - Gerador de relatórios;
  - Especialista em segurança;
  - Administrador de sistema;
  - Super usuário;
- 3.73 A solução deve suportar atribuição de usuários para as hierarquias:
  - Domínio raiz ou Grupo global;
  - Sub-domínios ou Sub-grupos;
  - Domínios ou Grupos superiores;
  - Domínios ou Grupos inferiores;
- 3.74 A solução deve suportar customização da console de gerência para exibir logo da empresa e mensagem aos usuários e administradores no momento da autenticação;
- 3.75 A solução deve suportar console de gerência no modelo Agentless, isto é, sem necessitar a instalação prévia de software de console de gerenciamento;
- 3.76 A solução deve suportar criação de ACL (Access Control List – Lista de Controle de Acesso), especificando quais endereços IP terão permissão de comunicação com a gerência;
- 3.77 A solução deve suportar comunicação entre gerência e equipamento criptografada, com as seguintes características:
  - SSL (Secure Sockets Layer) com RC4 e MD5 (Message-Digest algorithm 5);
  - SSL (Secure Sockets Layer) com MD5 (Message-Digest algorithm 5);
  - SSL (Secure Sockets Layer) de criptografia de 128-bit;
- 3.78 A solução deve suportar comunicação SNMPv3 (Simple Network Management Protocol Version 3) de 56-bit DES (Data Encryption Standard) e MD5 (Message-Digest algorithm 5);
- 3.79 A solução deve suportar terminal remoto a CLI (Command Line Interface) através de SSH (Secure Shell);
- 3.80 A solução deve suportar gerenciamento através de:
  - Gerência Centralizada – uma única instância de gerenciamento centralizado, não instância de Gerência Hierárquica;
  - Gerência Hierárquica – uma única instância de gerenciamento hierárquico é responsável por centralizar várias instâncias de Gerência Centralizada, sendo ela responsável por centralizar todas as funções de gerenciamento;
- 3.81 A solução deve suportar organização de equipamentos e ativos por grupos e sub-grupos hierárquicos, podendo-se incluir equipamentos, interfaces (físicas ou virtuais) ou grupo(s) de interfaces à um único grupo;
- 3.82 A solução deve suportar armazenamento em banco de dados relacional;
- 5.83 A solução deve suportar definição de políticas customizadas para:
  - Domínio raiz ou Grupo global;
  - Sub-domínios ou Sub-grupos;
  - Domínios ou Grupos superiores;
  - Domínios ou Grupos inferiores;
  - Equipamentos;
  - Interfaces físicas ou virtuais;
  - Grupo(s) de interfaces;
- 3.84 A solução deve suportar integração nativa com solução de Vulnerability Scanner (Análise de Vulnerabilidade) do mesmo fabricante do equipamento;



**ESTADO DE MATO GROSSO**  
**SECRETARIA DE ESTADO DO MEIO AMBIENTE**  
**SECRETARIA ADJUNTA DE GESTÃO SISTÊMICA**  
**COORDENADORIA DE AQUISIÇÕES E CONTRATOS**  
**GERENCIA DE FORMALIZAÇÃO DE CONTRATOS**

- 3.85 A solução deve suportar integração nativa com solução de HIPS (Host Intrusion Prevention System) do mesmo fabricante do equipamento;
- 3.86 A solução deve suportar integração nativa com solução de NTBA (Network Threat Behavior Analysis – Análise de Comportamento de Ameaça de Rede) do mesmo fabricante do equipamento;
- 3.87 A solução deve suportar integração nativa com solução de NAC (Network Access Control) do mesmo fabricante do equipamento;
- 3.88 A solução deve suportar integração nativa com solução de gerência de endpoints (estações de trabalho e notebooks) do mesmo fabricante do equipamento;
- 3.89 A solução deve suportar geração de alerta de no mínimo nove (09) níveis de severidade;
- 3.90 A solução deve suportar criação, configuração e manutenção de políticas diferenciadas por Virtual IPS por:
- Interface(s) física do equipamento;
  - Port Clustering, isto é, grupo(s) de interfaces físicas do equipamento;
  - Segmento(s) de monitoração e proteção;
  - Bloco(s) de endereços (CIDR – Classless Inter-Domain Routing);
  - VLAN Tagging 802.1Q;
- 3.91 A solução deve suportar atribuição de interfaces físicas ou virtuais, de um único equipamento, para diferentes grupos e/ou sub-grupos hierárquicos;
- 3.92 A solução deve suportar criação, configuração e manutenção de políticas diferenciadas por Port Clustering através do agrupamento de múltiplas interfaces físicas em uma única Virtual Interface, sendo também possível a criação, configuração e manutenção de políticas diferenciadas por Virtual IPS e Virtual Firewall pertencentes a uma única Virtual Interface;
- 3.93 A solução deve suportar edição, configuração e manutenção de evento e/ou múltiplos eventos, possibilitando-se ajuste granular:
- Deve suportar ajuste de assinaturas granular (On/Off);
  - Deve suportar ajuste de bloqueio granular (On/Off);
  - Deve suportar ajuste de severidade granular (Alta, Média, Baixa e Informativa);
  - Deve suportar ajuste de respostas granular;
- 3.94 A solução deve suportar busca por ataques, através da interface gráfica, por:
- Nome do ataque;
  - Aplicações impactadas pelo ataque;
  - Referências sobre o ataque através de nome completo ou REGEX, podendo ser através da identificação: ArachNIDS, BID (Bugtraq Identification), CERT (Computer Emergency Response Team), CVE (Common Vulnerability Exposure), Microsoft;
  - Novos ataques (atualização): Última atualização, Entre as atualizações X e Y, Entre as datas X e Y;
  - Família de equipamentos;
- 3.95 A solução deve suportar criação, configuração e manutenção de captura de tráfego;
- 3.96 A solução deve suportar políticas pré-configuradas específicas para os perfis:
- Interface interna do Firewall;
  - Interface externa do Firewall;
  - Segmento DMZ;
  - Segmento interno;
  - Servidor WEB;
  - Servidor Email;
  - Servidor DNS;
  - Servidor de arquivos;
  - Servidor Windows;
  - Servidor Solaris;
  - Servidor Unix;
  - Servidor Linux;
  - Bloqueio padrão de Intrusion Prevention System;



**ESTADO DE MATO GROSSO**  
**SECRETARIA DE ESTADO DO MEIO AMBIENTE**  
**SECRETARIA ADJUNTA DE GESTÃO SISTÊMICA**  
**COORDENADORIA DE AQUISIÇÕES E CONTRATOS**  
**GERENCIA DE FORMALIZAÇÃO DE CONTRATOS**

3.97 A solução deve suportar atribuição de políticas específicas e diferenciadas para tráfego Inbound e tráfego Outbound;

3.98 A solução deve suportar criação de regras e grupos de regras de Firewall através de:

- Endereço IP;
- Porta de comunicação;
- Protocolo de conexão;

3.99 A solução deve suportar visualização de customização para os ataques da política, através dos indicadores:

- Se o ataque foi customizado como parte de uma política Default;
- Se o ataque foi customizado através do editor de regras;
- Se o ataque foi customizado através do editor de políticas;
- Se o ataque foi customizado através de atualização configuração e atualização global;

3.100 A solução deve suportar visualização e classificação, ascendente e descendente, através das colunas:

- Ataque habilitado;
- Alerta habilitado;
- Nome do ataque;
- Número de identificação do ataque;
- Severidade;
- Customizado;
- Captura de pacotes;
- Ação de resposta;
- Bloqueio;
- Notificações;

3.101 A solução deve suportar funcionalidades de exportar (Export) e importar (Import) políticas;

3.102 A solução deve suportar múltiplas versões de políticas, assim como capacidade de comparação entre versões de uma mesma política ou de diferentes políticas;

3.103 A solução deve suportar controle de versão (Version Control) através de:

- Revisão da política;
- Data da política;
- Usuário que criou e/ou modificou a política;
- Descrição da política;
- Revisão ativa da política;

3.104 A solução deve suportar criação, configuração e manutenção de ACL (Access Control List – Política de Firewall), com as seguintes respostas:

- Allow: O tráfego é enviado Inline sem remontagem ou defragmentação dos pacotes;
- Allow + Intrusion Prevention: O tráfego é enviado Inline para remontagem dos pacotes;
- Drop: O tráfego será descartado, proporcionando um bloqueio dos pacotes;

3.105 A solução deve suportar TCP reset para:

- Origem do ataque;
- Destino do ataque;
- Origem e destino do ataque;

3.106 A solução deve suportar ICMP Host Unreachable;

3.107 A solução deve suportar bloqueio (Drop) de pacotes;

3.108 A solução deve suportar aplicação, extensão e remoção de quarentena (IPS Quarantine) sob demanda:

- Por um período de 15 minutos;
- Por um período de 30 minutos;
- Por um período de 45 minutos;
- Por um período de 60 minutos;
- Até remoção explícita;



**ESTADO DE MATO GROSSO**  
**SECRETARIA DE ESTADO DO MEIO AMBIENTE**  
**SECRETARIA ADJUNTA DE GESTÃO SISTÊMICA**  
**COORDENADORIA DE AQUISIÇÕES E CONTRATOS**  
**GERENCIA DE FORMALIZAÇÃO DE CONTRATOS**

- 3.109 A solução deve suportar lista de ataques recomendados para bloqueio, baseando esta lista em uma probabilidade de desencadeamento benígno, isto é, menor probabilidade de False-positive e False-negative;
- 3.110 A solução deve suportar ajuste de bloqueio inteligente, baseado em níveis de menor probabilidade de False-positive e False-negative;
- 3.111 A solução deve suportar configuração e atualização global de bloqueio para um ataque, propagando esta configuração e atualização em todas as políticas;
- 3.112 A solução deve suportar captura de pacotes para análise de evidências em formato PCAP (Packet Capture), permitindo:
- Visualização automática através do Wireshark;
  - Configuração do número de bytes em cada um dos pacotes a serem capturados: Captura de todo o pacote, Captura dos N primeiros bytes;
  - Configuração da duração da captura: Captura de somente os pacotes do ataque, Captura de N pacotes do ataque, Captura por tempo de duração do ataque, Captura do restante do fluxo do ataque;
- 3.113 A solução deve suportar envio de SNMP Trap, envio de e-mail, resposta definida pelo usuário (script), envio de alertas por PAGER e integração com ambiente de SYSLOG;
- 3.114 A solução deve suportar customização de cabeçalho e rodapé de relatórios, permitindo modificação de logo.
- 3.115 A solução deve suportar geração de relatórios:
- Baseados em modelos padrão, isto é, relatórios padrão;
  - Customizados pelo administrador e/ou usuário;
  - Agendados diária ou semanalmente;
  - Automáticos e enviados por e-mail para destinatários, diária ou semanalmente;
- 3.116 A solução deve suportar, no mínimo, trinta e seis (36) relatórios padrão, tais como:
- High Sensor TCP / UDP Flow Utilization;
  - High Sensor Throughput Utilization;
  - IPS Quarantine History;
  - System Health History;
  - System Health Summary;
  - Top 10 Applications Report;
  - Top 10 Attacks;
  - Top 10 Conversations Report;
  - Top 10 Host Traffic;
  - Top 10 Interface Traffic Report;
  - Top 10 Services Report;
  - ACL Assignments Report;
  - ACL Definitions Report;
  - Admin Domain and Users Report;
  - Attack Filters Report;
  - Faults Report;
  - Integration Summary Report;
  - Intrusion Policy Report;
  - IPS Configuration Summary Report;
  - IPS Policy Assignment Report;
  - IPS Policy Details Report;
  - IPS Sensor Report;
  - Manager Report;
  - Performance Monitoring - Admin Domain Configuration Report;
  - Performance Monitoring - Sensor Configuration Report;
  - Reconnaissance Policy Report;
  - Rule Set Report;





**ESTADO DE MATO GROSSO**  
**SECRETARIA DE ESTADO DO MEIO AMBIENTE**  
**SECRETARIA ADJUNTA DE GESTÃO SISTÊMICA**  
**COORDENADORIA DE AQUISIÇÕES E CONTRATOS**  
**GERENCIA DE FORMALIZAÇÃO DE CONTRATOS**

- Traffic Management Report;
- User Activity Report;
- Version Summary Report;
- Big Movers Report;
- Executive Summary Report;
- Malware Detection Report;
- Reconnaissance Attacks Report;
- Top N Attacks Report;
- Trend Analysis Report;

3.117 A solução deve suportar relatórios customizados pelo administrador e/ou usuário, permitindo, no mínimo, nove (9) campos de informação, tais como: - Grupos e sub-grupos hierárquicos; - Equipamento; - Interface; - Mecanismo de detecção; - Protocolo de conexão;

- Categoria; - Sub-categoria; - Endereço IP de origem; - Porta de comunicação de origem; - Endereço IP de destino; - Porta de comunicação de destino;

- Direção do ataque; - Severidade; - Relevância da vulnerabilidade; - Tipo de ataque; - Estado de alerta; - Ataques; - Campos de interesse;

- Tipo de organização;

3.118 A console de gerenciamento deverá ser totalmente compatível com a console para gerenciamento da McAfee e-Policy Orchestrator, já instalada e em funcionamento nesse órgão;

3.119 A solução deverá ter garantia de atualização por um período de 36 (trinta e seis) meses;

3.120 O fornecedor da solução deverá prestar suporte técnico on-site em até 04 horas úteis após a abertura do chamado, durante a vigência do contrato;

3.121 O fornecedor da solução deverá prestar suporte via e-mail e telefone 24 x 7 durante a vigência do contrato;

3.122 O fornecedor da solução realizará treinamento para utilização do produto, a ser ministrado fora das dependências do COLOG e Diretorias Subordinadas, e na cidade de Brasília-DF, para no mínimo 08 (oito) técnicos indicados pela Divisão de Tecnologia da Informação do COLOG e Diretorias Subordinadas, com 12 (doze) horas de duração em data e horários estabelecidos por este Departamento.

3.123 O COLOG e Diretorias Subordinadas, ao final do treinamento, passará uma pesquisa de satisfação com os participantes para verificar se os objetivos foram atingidos. Caso o índice mínimo não seja atingido o fornecedor repetirá o treinamento;

3.124 O fornecedor deverá providenciar atualização automática do produto mantendo-o sempre em sua última versão com todas as suas características, durante a vigência do contrato;

3.125 O fornecedor deverá providenciar a instalação e configuração da solução por técnico(s) certificado(s) pelo fabricante da solução;

3.126 O fornecedor deverá comprovar que o(s) técnico(s) possui(em) habilitação para executar os serviços de instalação, configuração e manutenção on-site, apresentando certificado técnico emitido pelo fabricante da solução, por ocasião da execução do serviço no COLOG e Diretorias Subordinadas;

3.127 O fornecedor deverá apresentar declaração do fabricante da solução ou do representante por esta indicado, de que a revenda está apta a prestar os serviços ofertados, com técnicos treinados e certificados bem como solidariedade do fabricante na implantação da solução proposta;

3.128 O fornecedor deverá apresentar no mínimo 01 (um) atestado de capacidade técnica de fornecimento da solução ofertada de pessoa de direito público ou privado.