

## **Projeto Básico**

### **Consulta Pública para aquisição de solução de NIPS (Network Intrusion Prevention System)**

#### **1.0 Objeto**

Consulta Pública para aquisição de solução de NIPS (Network Intrusion Prevention System) com inspeção de tráfego SSL e integração com ferramenta de análise de Vulnerabilidades e console de gerenciamento.

#### **2.0 Especificação do Objeto a ser Contratado**

Aquisição de dos seguintes itens para compor a solução de NIPS (Network Intrusion Prevention System):

##### **2.1 – ITEM I - SOLUÇÃO DE NETWORK IPS DE 3 GBPS COM INSPEÇÃO SSL E INTEGRAÇÃO COM ANÁLISE DE VULNERABILIDADES**

###### **2.1.1. Arquitetura de Hardware**

2.1.1.1. Possuir garantia de fim de linha dos equipamentos (End-Of-Life) que compõem a solução superior a 4 (quatro) anos após o aceite da solução.

2.1.1.2. Possuir Arquitetura específicas e desenvolvidas, tanto software quanto hardware, para as funcionalidades únicas, exclusivas e específicas dos Sistemas ofertados, para os serviços de NIPS e Inspeção SSL, não sendo permitido compor a solução, um equipamento de uso genérico. Os equipamentos que poderão ser de uso genérico estão relacionados aos serviços de Análise de Vulnerabilidades e Gerência.

2.1.1.3. Permitir visualização, no painel frontal, para fornecer informações sobre o equipamento (AMOSTRA).

2.1.1.4. Suportar fonte de energia tanto para Corrente Alternada ou Alternada (AC – Alternating Current) quanto para Corrente Contínua ou Galvânica (DC – Direct Current).

2.1.1.5. Possuir duas fontes de alimentação “Hot-swap/Hot-plug” com chaveamento automático e capacidade de operar em tensões de 100 a 240V, 50-60Hz. O equipamento deverá ser capaz de funcionar em sua totalidade, com somente uma das duas fontes fornecidas (AMOSTRA).

###### **2.1.2. Desempenho e Escalabilidade**

2.1.2.1. Permitir operação em modo Full-Duplex e Half-Duplex, suportando uma análise de tráfego agregado total de 3 Gbps, sem utilização de agregador de tráfego ou equipamento externo para balanceamento de tráfego (AMOSTRA).

2.1.2.2. Suportar no mínimo 1.000.000 (um milhão) de conexões concorrentes e taxa de 30.000 (trinta mil) novas conexões por segundo (AMOSTRA).

2.1.2.3. Suportar taxa de SYN Cookie de pelo menos 1.000.000 (um milhão) de pacotes TCP SYN por segundo com tamanho de 64 bytes.

2.1.2.4. Agregar latência de no máximo 150 µs (cento e cinquenta microssegundos) considerando tráfego com pacotes UDP com tamanho de 64 bytes, de acordo com especificações da RFC 2544 (AMOSTRA).

2.1.2.5. Permitir análise de tráfego HTTPS (HyperText Transfer Protocol Secure), isto é, conexões seguras com criptografia SSL (Secure Sockets Layer) em servidores WEB utilizando certificados PKCS12 (extensões “.pkcs12”, “.p12”, ou “.pfx”), nas versões SSLv2, SSLv3 e TLS e com codificações RC4, DES, 3DES e AES. Esta funcionalidade pode ser realizada em appliance externo, desde que possua o mesmo sistema de gerência e não haja prejuízo das demais especificações (AMOSTRA).

2.1.2.6. Suportar análise de tráfego SSL (Secure Sockets Layer) de no mínimo 1 Gbps (a análise deve permitir a inspeção decifrada de todo o conteúdo do pacote). Esta funcionalidade pode ser realizada em equipamento externo, desde que possua o mesmo sistema de gerência e não haja prejuízo das demais especificações (AMOSTRA).

2.1.2.7. Suportar pelo menos 60 (sessenta) certificados importados para análise de tráfego SSL (Secure Sockets Layer) (AMOSTRA).

- 2.1.2.8. Suportar no mínimo 90.000 (noventa mil) fluxos SSL (Secure Sockets Layer) (AMOSTRA).
- 2.1.2.9. Suportar administração, configuração e manutenção de no mínimo:
- 2.1.2.9.1. Perfis de DoS (Denial of Service – Negação de Serviço).
- 2.1.2.9.2. Regras de ACL (Access Control List – Lista de Controle de Acesso).
- 2.1.2.9.3. Virtual IPS (Intrusion Prevention System – Sistema de Prevenção de Intrusão) por meio de sub-interfaces. IPS virtuais podem ser configurados por VLAN (IEEE 802.1Q), VLAN Bridging (Pairing) e/ou CIDR (Classless Inter-Domain Routing).
- 2.1.2.10. Suportar no mínimo 8 (oito) interfaces Gigabit Ethernet “Hot-plug” para cabeamentos: Cobre (10BASE-T/100BASE-TX/1000BASE-T), Fibra multimodo (1000BASE-SX) e Fibra monomodo (1000BASE-LX).
- 2.1.2.11. Suportar no mínimo 4 (quatro) interfaces 10-Gigabit Ethernet “Hot-plug” para cabeamentos: Fibra multimodo (10GBASE-SR) e Fibra monomodo (10GBASE-LR).
- 2.1.2.12. Possuir equipamento de By-pass (Fail-open), externo ou interno, integrado ao equipamento de NIPS, não afetando o tráfego de rede em caso de falha das interfaces (AMOSTRA).
- 2.1.2.13. Possuir interface adicional Gigabit Ethernet, para cabeamentos Cobre (10BASE-T/100BASE-TX/1000BASE-T), exclusiva e dedicada para gerência.
- 2.1.2.14. Possuir uma interface Gigabit Ethernet, para cabeamentos Cobre (10BASE-T/100BASE-TX/1000BASE-T), exclusiva e dedicada para envio de respostas.
- 2.1.2.15. Possuir interface dedicada para conexão a console.

## **2.2 – ITEM II - SOLUÇÃO DE NETWORK IPS DE 10 GBPS COM INSPEÇÃO SSL E INTEGRAÇÃO COM ANÁLISE DE VULNERABILIDADES**

### **2.2.1. Arquitetura de Hardware**

- 2.2.1.1. Possuir garantia de fim de linha dos equipamentos (End-Of-Life) que compõem a solução superior a 4 (quatro) anos após o aceite da solução.
- 2.2.1.2. Possuir Arquitetura específicas e desenvolvidas, tanto software quanto hardware, para as funcionalidades únicas, exclusivas e específicas dos Sistemas ofertados, para os serviços de NIPS e Inspeção SSL, não sendo permitido compor a solução , um equipamento de uso genérico. Os equipamentos que poderão ser de uso genérico estão relacionados aos serviços de Análise de Vulnerabilidades e Gerência.
- 2.2.1.3. Permitir visualização, no painel frontal, para fornecer informações sobre o equipamento (AMOSTRA).
- 2.2.1.4. Suportar fonte de energia tanto para Corrente Alternada ou Alternada (AC – Alternating Current) quanto para Corrente Contínua ou Galvânica (DC – Direct Current).
- 2.2.1.5. Possuir duas fontes de alimentação “Hot-swap/Hot-plug” com chaveamento automático e capacidade de operar em tensões de 100 a 240V, 50-60Hz. O equipamento deverá ser capaz de funcionar em sua totalidade, com somente uma das duas fontes fornecidas (AMOSTRA).

### **2.2.2. Desempenho e Escalabilidade**

- 2.2.2.1. Permitir operação em modo Full-Duplex e Half-Duplex, suportando uma análise de tráfego agregado de 10 Gbps, sem utilização de agregador de tráfego ou equipamento externo para balanceamento de tráfego (AMOSTRA).
- 2.2.2.2. Suportar no mínimo 4.000.000 (quatro milhões) de conexões concorrentes. e no mínimo 120.000 (cento e vinte mil) novas conexões por segundo (AMOSTRA).
- 2.2.2.3. Suportar taxa de SYN Cookie de pelo menos 4.000.000 (quatro milhões) de pacotes TCP SYN por segundo com tamanho de 64 bytes.
- 2.2.2.4. Agregar latência de no máximo 150 µs (cento e cinquenta microssegundos) considerando tráfego com pacotes UDP com tamanho de 64 bytes, de acordo com especificações da RFC 2544 (AMOSTRA).
- 2.2.2.5. Permitir análise de tráfego HTTPS (HyperText Transfer Protocol Secure), isto é, conexões seguras com criptografia SSL (Secure Sockets Layer) em servidores WEB utilizando certificados PKCS12 (extensões “.pkcs12”, “.p12”, ou “.pfx”), nas versões SSLv2, SSLv3 e TLS e

com codificações RC4, DES, 3DES e AES. Esta funcionalidade pode ser realizada em appliance externo, desde que possua o mesmo sistema de gerencia e não haja prejuízo das demais especificações (AMOSTRA).

2.2.2.6. Suportar análise de tráfego SSL (Secure Sockets Layer) de no mínimo 3 Gbps (a análise deve permitir a inspeção decifrada de todo o conteúdo do pacote). Esta funcionalidade pode ser realizada em equipamento externo, desde que possua o mesmo sistema de gerencia e não haja prejuízo das demais especificações (AMOSTRA).

2.2.2.7. Suportar pelo menos 60 certificados importados para análise de tráfego SSL (Secure Sockets Layer) (AMOSTRA).

2.2.2.8. Suportar no mínimo 300.000 (trezentos mil) fluxos SSL (Secure Sockets Layer) (AMOSTRA).

2.2.2.9. Suportar administração, configuração e manutenção de no mínimo:

2.2.2.9.1. Perfis de DoS (Denial of Service – Negação de Serviço).

2.2.2.9.2. Regras de ACL (Access Control List – Lista de Controle de Acesso).

2.2.2.9.3. Virtual IPS (Intrusion Prevention System – Sistema de Prevenção de Intrusão) por meio de sub-interfaces. IPS virtuais podem ser configurados por VLAN (IEEE 802.1Q), VLAN Bridging (Pairing) e/ou CIDR (Classless Inter-Domain Routing).

2.2.2.10. Suportar no mínimo 8 (oito) interfaces Gigabit Ethernet “Hot-plug” para cabeamentos: Cobre (10BASE-T/100BASE-TX/1000BASE-T), Fibra multimodo (1000BASE-SX) e Fibra monomodo (1000BASE-LX).

2.2.2.11. Suportar no mínimo 6 (seis) interfaces 10-Gigabit Ethernet “Hot-plug” para cabeamentos: Fibra multimodo (10GBASE-SR) e Fibra monomodo (10GBASE-LR).

2.2.2.12. Possuir equipamento de By-pass (Fail-open), externo ou interno, integrado ao equipamento de NIPS, não afetando o tráfego de rede em caso de falha das interfaces (AMOSTRA).

2.2.2.13. Possuir interface adicional Gigabit Ethernet, para cabeamentos Cobre (10BASE-T/100BASE-TX/1000BASE-T), exclusiva e dedicada para gerência.

2.2.2.14. Possuir uma interface Gigabit Ethernet, para cabeamentos Cobre (10BASE-T/100BASE-TX/1000BASE-T), exclusiva e dedicada para envio de respostas.

2.2.2.15. Possuir interface dedicada para conexão a console.

## **2.3 – ITEM 3 - SOLUÇÃO DE NETWORK IPS DE 20 GBPS COM INSPEÇÃO SSL E INTEGRAÇÃO COM ANÁLISE DE VULNERABILIDADES**

### **2.3.1. Arquitetura de Hardware**

2.3.1.1. Possuir garantia de fim de linha dos equipamentos (End-Of-Life) que compõem a solução superior a 4 (quatro) anos após o aceite da solução.

2.3.1.2. Possuir Arquitetura específicas e desenvolvidas, tanto software quanto hardware, para as funcionalidades únicas, exclusivas e específicas dos Sistemas ofertados, para os serviços de NIPS e Inspeção SSL, não sendo permitido compor a solução, um equipamento de uso genérico. Os equipamentos que poderão ser de uso genérico estão relacionados aos serviços de Análise de Vulnerabilidades e Gerência.

2.3.1.3. Permitir visualização, no painel frontal, para fornecer informações sobre o equipamento (AMOSTRA).

2.3.1.4. Suportar fonte de energia tanto para Corrente Alternada ou Alternada (AC – Alternating Current) quanto para Corrente Contínua ou Galvânica (DC – Direct Current).

2.3.1.5. Possuir duas fontes de alimentação “Hot-swap/Hot-plug” com chaveamento automático e capacidade de operar em tensões de 100 a 240V, 50-60Hz. O equipamento deverá ser capaz de funcionar em sua totalidade, com somente uma das duas fontes fornecidas (AMOSTRA).

### **2.3.2. Desempenho e Escalabilidade**

2.3.2.1. Permitir operação em modo Full-Duplex e Half-Duplex, suportando uma análise de tráfego agregado de 20 Gbps, sem utilização de agregador de tráfego ou equipamento externo para balanceamento de tráfego (AMOSTRA).

2.3.2.2. Suportar no mínimo 6.000.000 (seis milhões) de conexões concorrentes. e no mínimo

200.000 (duzentas mil) novas conexões por segundo (AMOSTRA).

2.3.2.3. Suportar taxa de SYN Cookie de pelo menos 6.000.000 (seis milhões) de pacotes TCP SYN por segundo com tamanho de 64 bytes.

8.4. Agregar latência de no máximo 150 µs (cento e cinquenta microssegundos) considerando tráfego com pacotes UDP com tamanho de 64 bytes, de acordo com especificações da RFC 2544 (AMOSTRA).

2.3.2.5. Permitir análise de tráfego HTTPS (HyperText Transfer Protocol Secure), isto é, conexões seguras com criptografia SSL (Secure Sockets Layer) em servidores WEB utilizando certificados PKCS12 (extensões “.pkcs12”, “.p12”, ou “.pfx”), nas versões SSLv2, SSLv3 e TLS e com codificações RC4, DES, 3DES e AES. Esta funcionalidade pode ser realizada em appliance externo, desde que possua o mesmo sistema de gerência e não haja prejuízo das demais especificações (AMOSTRA).

2.3.2.6. Suportar análise de tráfego SSL (Secure Sockets Layer) de no mínimo 6 Gbps (a análise deve permitir a inspeção decifrada de todo o conteúdo do pacote, porém mantendo-se a confidencialidade do tráfego). Esta funcionalidade pode ser realizada em equipamento externo, desde que possua o mesmo sistema de gerência e não haja prejuízo das demais especificações (AMOSTRA).

2.3.2.7. Suportar pelo menos 60 (sessenta) certificados importados para análise de tráfego SSL (Secure Sockets Layer) (AMOSTRA).

2.3.2.8. Suportar no mínimo 600.000 (seiscentos mil) fluxos SSL (Secure Sockets Layer) (AMOSTRA).

2.3.2.9. Suportar administração, configuração e manutenção de no mínimo:

2.3.2.9.1. Perfis de DoS (Denial of Service – Negação de Serviço).

2.3.2.9.2. Regras de ACL (Access Control List – Lista de Controle de Acesso).

2.3.2.9.3. Virtual IPS (Intrusion Prevention System – Sistema de Prevenção de Intrusão) por meio de sub-interfaces. IPS virtuais podem ser configurados por VLAN (IEEE 802.1Q), VLAN Bridging (Pairing) e/ou CIDR (Classless Inter-Domain Routing).

2.3.2.10. Suportar no mínimo 8 (oito) interfaces Gigabit Ethernet “Hot-plug” para cabeamentos: Cobre (10BASE-T/100BASE-TX/1000BASE-T), Fibra multimodo (1000BASE-SX) e Fibra monomodo (1000BASE-LX).

2.3.2.11. Suportar no mínimo 6 (seis) interfaces 10-Gigabit Ethernet “Hot-plug” para cabeamentos: Fibra multimodo (10GBASE-SR) e Fibra monomodo (10GBASE-LR).

2.3.2.12. Possuir equipamento de By-pass (Fail-open), externo ou interno, integrado ao equipamento de NIPS, não afetando o tráfego de rede em caso de falha das interfaces (AMOSTRA).

2.3.2.13. Possuir interface adicional Gigabit Ethernet, para cabeamentos Cobre (10BASE-T/100BASE-TX/1000BASE-T), exclusiva e dedicada para gerência.

2.3.2.14. Possuir uma interface Gigabit Ethernet, para cabeamentos Cobre (10BASE-T/100BASE-TX/1000BASE-T), exclusiva e dedicada para envio de respostas.

2.3.2.15. Possuir interface dedicada para conexão a console.

## **2.4 – ITEM IV - INTERFACES 1GE (GIGABIT ETHERNET) E 10GE (10 GIGABIT ETHERNET) PARA SOLUÇÕES DE NETWORK IPS**

2.4.1. Interfaces 1Ge (Gigabit Ethernet)

2.4.1.1. Interfaces 1Ge (Gigabit Ethernet) “Hot-plug” para cabeamentos:

2.4.1.1.1. Cobre (10BASE-T/100BASE-TX/1000BASE-T).

2.4.1.1.2. Fibra multimodo (1000BASE-SX).

2.4.1.1.3. Fibra monomodo (1000BASE-LX).

2.4.2. Interfaces 10Ge (10 Gigabit Ethernet)

2.4.2.1. Interfaces 10Ge (10 Gigabit Ethernet) “Hot-plug” para cabeamentos:

2.4.2.1.1. Fibra multimodo (10GBASE-SR).

2.4.2.1.2. Fibra monomodo (10GBASE-LR).

## **2.5 – ITEM V - ESPECIFICAÇÃO TECNOLÓGICA PARA SOLUÇÕES DE NETWORK IPS DE 3**

## **GBPS, 10 GBPS E 20 GBPS**

### **2.5.1. Modos de Operação**

2.5.1.1. Suportar, em um único equipamento, quaisquer combinações dos seguintes modos de operação: Inline (Fail-open e Fail-close), Port Mirroring/SPAN, TAP, Grupo de interfaces (Port Clustering) e VLAN.

2.5.1.2. Suportar instalação sem necessidade de reconfiguração de roteadores e switches, quando no modo de operação Inline Mode (AMOSTRA).

2.5.1.3. Suportar monitoração e proteção de segmentos de rede em modo transparente e operação na camada 2 do modelo OSI. Isto é, as interfaces de monitoração e proteção não possuem endereço IP nem endereço MAC (AMOSTRA).

2.5.1.4. Suportar auto-negociação, conforme especificação IEEE 802.3u, ou configuração manual de velocidade para todas as interfaces do equipamento.

2.5.1.5. Suportar instalação de modo Inline, sem bloqueio para ataques. Isto é, quando instalado em modo Inline o equipamento pode ser configurado para não bloquear ataques específicos ou todos os ataques, apenas gerando alertas.

2.5.1.6. Suportar instalação em modo de operação de alta-disponibilidade (conforme descrito no item 2.5.1).

2.5.1.7. Suportar funcionamento como Firewall transparente, permitindo a criação de regras para filtros de acesso de camada 3 do modelo OSI.

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

2.5.1.9. Suportar configuração flexível “pass-through” para tráfego que ultrapasse a análise de tráfego agregado suportado pelos equipamentos (conforme descrito nos itens 2.1.1.1, 2.1.2.1 e 2.3.1.1) (AMOSTRA).

2.5.1.10. Suportar configuração flexível de exceções de monitoração de tráfego de VLAN, TCP e UDP, que não deverá ser analisado e contabilizado no tráfego agregado suportado pelo equipamento, isto é, quando criada uma exceção de monitoração de tráfego de uma VLAN a qual gere, por exemplo, 5 Gbps de tráfego, estes 5 Gbps serão excluídos da monitoração e não serão decrementados do tráfego agregado suportado pelo equipamento (conforme descrito nos itens 2.1.1.1, 2.1.2.1 e 2.3.1.1), permitindo gerência de exceções de tráfego (AMOSTRA).

2.5.1.11. Suportar configuração flexível permitindo selecionar o tráfego indesejado a ser ignorado pela análise e monitoração IPS com base na origem, destino e protocolo.

### **2.5.2. Detecção de Ataques**

2.5.2.1. Suportar análise e decodificação de no mínimo 200 (duzentos) protocolos de rede entre a camada 2 e a camada 7 do modelo OSI.

2.5.2.2. Suportar decodificação e/ou normalização de campos de cabeçalho inválidos, pacotes mal formatados, pacotes anômalos em conformidade com RFCs e/ou especificações dos protocolos, para no mínimo: IEEE 802.2, 3GPP TS 29.060, 3GPP TS 29.274, 3GPP TS 32.295, CVS, DCE/RPC, MS-SQLR 6.0, EIGRP, IEEE 802.1Q, IEEE 802.3, ITU-T H.225.0, ITU-T H.323, MS-NBTE 10.0, MS-RAIW 6.0, MS-TDS 12.0, MS-WINSRA 10.0, NHRP, RFC 1001, RFC 1002, RFC 1032, RFC 1033, RFC 1034, RFC 1035, RFC 1050, RFC 1057, RFC 1064, RFC 1071, RFC 1094, RFC 1101, RFC 1112, RFC 1122, RFC 1123, RFC 1176, RFC 1178, RFC 1183, RFC 1203, RFC 1288, RFC 1413, RFC 1534, RFC 1542, RFC 1579, RFC 1591, RFC 1639, RFC 1716, RFC 1813, RFC 1831, RFC 1833, RFC 1912, RFC 1945, RFC 1995, RFC 1996, RFC 2068, RFC 2131, RFC 2132, RFC 2228, RFC 2236, RFC 2389, RFC 2407, RFC 2408, RFC 2409, RFC 2460, RFC 2563, RFC 2610, RFC 2616, RFC 2640, RFC 2683, RFC 2710, RFC 3010, RFC 3011, RFC 3046, RFC 3074, RFC 3118, RFC 3203, RFC 3376, RFC 3501, RFC 3530, RFC 3659, RFC 3810, RFC 4314, RFC 4443, RFC 4604, RFC 5531, RFC 5661, RFC 5797, RFC 5797, RFC 697, RFC 742, RFC 760, RFC 791, RFC 792, RFC 882, RFC 883, RFC 912, RFC 920, RFC 931, RFC 951, RFC 768, RFC 793, RFC 1323, RFC 2018, RFC 959 e SCCP.

2.5.2.3. Suportar tanto análise Stateful Inspection, mantendo o estado das sessões monitoradas, quanto Stateless Inspection.

- 2.5.2.4. Suportar administração, configuração e manutenção de ACL em camada 3, com as seguintes respostas:
- 2.5.2.4.1. Permitir: O tráfego é enviado Inline sem remontagem dos pacotes.
  - 2.5.2.4.2. Permitir + Prevenir Ataques: O tráfego é enviado Inline para remontagem dos pacotes.
  - 2.5.2.4.3. Descartar: O tráfego será descartado.
- 2.5.2.5. Suportar criação de objetos de rede e/ou máquinas (servidores e estações de trabalho) para agrupamento destes em regras de controle de acesso (ACL) (AMOSTRA).
- 2.5.2.6. Suportar detecção e bloqueio de ataques, no mínimo, das seguintes modalidades:
- 2.5.2.6.1. Inspeção de tráfego Stateful: IP defragmentation e TCP stream reassembly.
  - 2.5.2.6.2. Anomalias.
  - 2.5.2.6.3. Por assinaturas: Definidas pelo fabricante, Definidas pelo usuário e Open-source.
  - 2.5.2.6.4. Detecção heurística de Botnet.
  - 2.5.2.6.5. Correlação multi-ataque.
  - 2.5.2.6.6. Por protocolos de camada 7 do modelo OSI.
  - 2.5.2.6.7. Quarentena de máquinas. (O atacante deverá ficar bloqueado temporariamente no equipamento em questão).
  - 2.5.2.6.8. Proteção contra tentativa de evasão.
  - 2.5.2.7. Permitir proteção efetiva contra técnicas de evasão.
  - 2.5.2.8. Suportar detecção e bloqueio de ataques independente do sistema operacional alvo.
  - 2.5.2.9. Suportar identificação passiva dos sistemas operacionais (Passive OS Fingerprint) dos sistemas monitorados dos segmentos protegidos.
  - 2.5.2.10. Suportar análise de tráfego na direção servidor-cliente, isto é, ataques originados externamente e direcionados à clientes e/ou usuários internos ("Client-side Attacks" ou "Drive-by Attacks") (AMOSTRA).
  - 2.5.2.11. Suportar detecção e bloqueio de ataques direcionados à servidores de aplicação WEB, através de tecnologia heurística, isto é, detecção heurística e bloqueio de ataques SQL Injection (AMOSTRA).
  - 2.5.2.12. Suportar detecção heurística de atividades de agentes (zumbis) internos que pertençam a Botnet.
  - 2.5.2.13. Suportar administração, configuração e manutenção de controle de limites de conexões (Connection Limiting) ou bloqueio, para no mínimo:
    - 2.5.2.13.1. Direção: Inbound, Outbound e Bidirecional (AMOSTRA).
    - 2.5.2.13.2. Tipo de Regra: Baseada em Protocolo (AMOSTRA).
  - 2.5.2.14. Suportar detecção e bloqueio de Shellcodes direcionados às plataformas e famílias de CPUs específicas, para no mínimo: HP PA-RISC Family CPU, Intel Alpha Family CPU, MIPS Family CPU, i386 Family CPU, Motorola 68000 Family CPU, PowerPC Family CPU e SPARC Family.
  - 2.5.2.15. Suportar as categorias de ataques e tipos de ameaças, para no mínimo:
    - 2.5.2.15.1. Reconnaissance: Brute Force, Host Sweep, OS Fingerprinting, Port Scan e Service Sweep.
    - 2.5.2.15.2. Exploits: Arbitrary Command Execution, Backdoor, Bot, Buffer Overflow, Denial of Service, DDoS Agent Activity, Code/Script Execution, Evasion Attempt, Privileged Access, Probe, Protocol Violation, Remote Access, Shellcode Execution, Trojan, Virus, Read Exposure, Worms e Write Exposure.
    - 2.5.2.15.3. Volume DoS: Statistical Deviation e Over Threshold.
    - 2.5.2.15.4. Policy Violations: Audit, Command Shell, Covert Channel, Non-standard Port, Phising, PuP (Potential Unwanted Program), Restricted Access, Restricted Application, Sensitive Content e Unauthorized IP.
  - 2.5.2.16. Suportar assinaturas para detecção e bloqueio de ataques através de vulnerabilidades DoS (Denial of Service), para no mínimo: Bonk Attack, Jolt Attack, Land Attack, Ping of Death Attack, Newtear Attack e Teardrop Attack (AMOSTRA).
  - 2.5.2.17. Suportar assinaturas para detecção e bloqueio de atividades de agentes (zumbis)

DDoS (Distributed Denial of Service), para no mínimo: Trinoo, Tribal Flood Network (TFN), TFN2K, Stacheldraht, Shaft, Trinity e Mstream.

2.5.2.18. Suportar detecção e bloqueio baseado em modo aprendizagem (Learning Mode), através de anomalias estatísticas (Statistical Anomalies) e desequilíbrio do tráfego, para Flood (Volume) DoS Attacks, para no mínimo: TCP SYN, TCP Full Connect, TCP ACK/FIN, TCP RST, DNS Flood, UDP Flood e ICMP Flood (AMOSTRA).

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

2.5.2.20. Suportar detecção e bloqueio para conexões P2P (Peer-to-Peer) evasivas que utilizem transferências de arquivos criptografadas e/ou com técnicas de “Obfuscated Binary”.

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

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

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

### **2.5.3. Respostas**

2.5.3.1. Suportar TCP Reset para origem do ataque, destino do ataque e, origem e destino do ataque (AMOSTRA).

2.5.3.2. Suportar ICMP Host Unreachable (AMOSTRA).

2.5.3.3. Suportar bloqueio (Drop) de pacotes (AMOSTRA).

2.5.3.4. Suportar aplicação, extensão e remoção de quarentena (IPS Quarantine) sob demanda por períodos programáveis e por remoção explícita (AMOSTRA).

2.5.3.5. Suportar ajuste de bloqueio inteligente, baseado em assinaturas recomendadas pelo fabricante para bloqueio (AMOSTRA).

2.5.3.6. Suportar configuração e atualização global de bloqueio para um ataque, propagando esta configuração e atualização em todas as políticas.

2.5.3.7. Suportar captura de pacotes para análise de evidências em formato LIBPCAP (Library for Packet Capture) (AMOSTRA).

2.5.3.8. Suportar envio de SNMP Trap.

2.5.3.9. Suportar envio de e-mail.

2.5.3.10. Suportar resposta definida pelo usuário (Script).

2.5.3.11. Suportar integração com ambiente de SYSLOG.

### **2.5.4. Alta-disponibilidade**

2.5.4.1. Stateful Fail-over: utilizando-se dois equipamentos, possibilitando a implementação de Alta-disponibilidade, mantendo os estados das sessões, em um ambiente configurado com roteamento simétrico. Os equipamentos operam sendo um ativo e outro passivo.

2.5.4.2. Load-balance: utilizando-se dois equipamentos, possibilitando a implementação de Alta-disponibilidade, mantendo os estados das sessões, em um ambiente configurado com roteamento assimétrico (balanceamento de carga). Os equipamentos podem operar em modo ativo/ativo ou ativo/passivo.

2.5.4.3. Stateful Fail-open: utilizando-se dois equipamentos, possibilitando a implementação de Alta-disponibilidade, mantendo os estados das sessões, em um ambiente configurado com roteamento simétrico ou roteamento assimétrico (balanceamento de carga). Os equipamentos podem operar em modo ativo/ativo ou ativo/passivo.

### **2.5.5. Imunidade a Tentativa de Evasão**

2.5.5.1 Possuir técnica de detecção e prevenção contra evasão por ofuscação de URL

2.5.5.2 Possuir técnica de detecção e prevenção contra evasão por segmentação TCP

### **2.5.6. Integração com Análise de Vulnerabilidades**

2.5.6.1. Deve possuir solução de análise de vulnerabilidades, interna ou externa ao equipamento de NIPS, desde que não haja perda da performance mínima exigida para a função principal de NIPS.

2.5.6.2. Suportar modos de integração, para no mínimo:

2.5.6.2.1. Automática: Importação automática e agendada de resultados de análise de vulnerabilidades.

2.5.6.2.2. Manual: Importação manual de resultados de análise de vulnerabilidades.

2.5.6.3. Suportar demonstração de informações detalhadas dos ativos de rede, tanto para origem quanto para o destino, através de correlação de ataques e vulnerabilidades, para no mínimo:

2.5.6.3.1. Sistema Operacional do ativo de rede (AMOSTRA).

2.5.6.3.2. Service Pack do ativo de rede (AMOSTRA).

2.5.6.3.3. Portas de comunicação abertas e ativas no ativo de rede (AMOSTRA).

2.5.6.3.4. Protocolos de comunicação disponíveis no ativo de rede (AMOSTRA).

2.5.6.3.5. Serviços disponível no ativo de rede.

2.5.6.3.6. Lista de vulnerabilidades do ativo de rede.

2.5.6.3.7. Lista de vulnerabilidades em aplicações web.

2.5.6.4. Suportar correlação de informações sobre a relevância do ataque.

## **2.6 – ITEM VI - CONSOLE DE GERENCIA DE SOLUÇÃO NETWORK IPS E INSPEÇÃO DE TRAFEGO SSL**

### **2.6.1. Gerenciamento**

2.6.1.1. Possuir políticas com assinaturas recomendadas pelo fabricante para bloqueio, as quais são baseadas nas recomendações provenientes de equipe de pesquisa do fabricante (AMOSTRA).

2.6.1.2. Deve permitir console de gerência no modelo “Agent-less”, isto é, não há necessidade de instalação de software de console de gerenciamento (AMOSTRA).

2.6.1.3. Deve permitir atualização e aplicação de políticas de segurança, através da gerência, sem afetar tanto a detecção quanto o bloqueio, isto é, o equipamento gerenciado não perderá capacidade de detecção e bloqueio durante o processo de atualização de políticas e regras (AMOSTRA).

2.6.1.4. Deve permitir atualização de novas versões, tanto de firmware quanto de assinaturas, sem necessidade de reinicialização do equipamento gerenciado.

2.6.1.5. Deve permitir customização de “Dashboards” para visualização resumida de eventos (AMOSTRA).

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

2.6.1.7. Deve permitir instalação em HA (High Availability – Alta-disponibilidade) ativo-passivo.

2.6.1.8. Deve permitir modos heterogêneos de atualização, para no mínimo:

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

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

2.6.1.9. Deve permitir autenticação de usuários, administradores e monitores por meio de:

2.6.1.9.1. Autenticação local: usuários e administradores cadastrados na gerência, permitindo definir políticas de composição de senhas (AMOSTRA).

2.6.1.9.2. Autenticação LDAP, permitindo SSL (Secure Sockets Layer) e Non-SSL (Secure Sockets Layer) (AMOSTRA).

2.6.1.9.3. Autenticação RADIUS, permitindo PAP (Password Authentication Protocol), CHAP



(Challenge Handshake Authentication Protocol) e EAP-MD5 (Extensible Authentication Protocol-MD5) (AMOSTRA).

2.6.1.10. Deve permitir atribuição de perfis para usuário, administradores e monitores com níveis de permissão diferenciados (AMOSTRA).

2.6.1.11. Deve permitir atribuição de usuários de forma hierárquica, isto é, deve ser possível restringir a gerência para determinados grupos (AMOSTRA).

2.6.1.12. Deve permitir customização da console de gerência para exibir logo da empresa e mensagem aos usuários e administradores no momento da autenticação.

2.6.1.13. Suportar criação de ACL (Access Control List – Lista de Controle de Acesso), através da Console de Gerência, especificando quais endereços IP terão permissão de comunicação com a gerência (AMOSTRA).

2.6.1.14. Deve permitir comunicação entre gerência e equipamento de forma criptografada.

2.6.1.15. Deve permitir SNMPv3 (Simple Network Management Protocol Version 3) de 56-bit DES (Data Encryption Standard) e MD5 (Message-Digest algorithm 5).

2.6.1.16. Deve permitir terminal remoto CLI (Command Line Interface) por meio de SSH (Secure Shell).

2.6.1.16.1. Deve permitir organização de equipamentos e ativos por grupos e subgrupos hierárquicos, podendo-se incluir equipamentos, interfaces (físicas ou virtuais), grupo(s) de interfaces de um único equipamento e/ou grupo de interfaces de equipamentos distintos (AMOSTRA).

2.6.1.17. Deve permitir definição de políticas customizadas por grupos: de equipamentos e interfaces físicas ou virtuais (AMOSTRA).

2.6.1.18. Deve permitir integração, através de SNMPv3, com solução de Sistema de Gerenciamento de Rede (AMOSTRA).

2.6.1.19. Fornecer arquivo MIB (SNMPv3) para integração com solução de Sistema de Gerenciamento de Rede (AMOSTRA).

2.6.1.20. A solução de console deverá possuir quantidade de memória e processamento mínima suficiente para atendimento de todas as funcionalidades e desempenho solicitados neste documento.

2.6.1.21. Deverá possuir no mínimo 06 (seis) TB de armazenamento local em disco de pelo menos 10K RPM (AMOSTRA).

2.6.1.22. Os Discos de armazenamento deverão possuir redundância em RAID 5 ou 6 (AMOSTRA).

2.6.1.23. O Equipamento deverá possuir fontes redundantes internas do tipo “Hot-swap/Hot-plug”, com capacidade para suportar toda a solução, sem perda de capacidade ou funcionalidade, no caso de falha das fontes principais (AMOSTRA).

## 2.7. Da Quantidade

ITEM	DESCRIÇÃO	QUANTIDADE
ITEM I	Solução NIPS 03 Gb	22
ITEM II	Solução NIPS 10 Gb	10
ITEM III	Solução NIPS 20 Gb	10
ITEM IV	Interfaces 1Gbe	216
ITEM IV	Interfaces 10Gbe	60
ITEM V	Especificação Técnica	Não Se Aplica
ITEM VI	Console de Gerência	04 Clusters (8 equipamentos)

## 2.8. Da Operacionalização da Solução

2.8.1. Faculta-se o SERPRO e a Contratada, sempre quando necessário, agendar reuniões

periódicas de caráter gerencial e/ou técnico para avaliar os trabalhos, adotar resoluções e obter esclarecimento de pendências durante toda a vigência do contrato e garantia.

2.8.2. O SERPRO se reserva no direito de remanejar a solução contratada entre suas Regionais e Escritórios, no Território Nacional.

## **2.9. Da Entrega e do Prazo de Entrega**

2.9.1. Entende-se por cumprimento do prazo de entrega o recebimento dos componentes da solução, sua instalação e execução dos serviços no SERPRO, deixando-os operacionais para o aceite definitivo. O não cumprimento rigoroso do prazo de entrega, ou entrega parcial, ou entrega de configuração inferior a solicitada implicará em rescisão do contrato a ser firmado entre o SERPRO e a contratada.

2.9.2. A solução com seus componentes adquiridos no edital, bem como os softwares básicos, os serviços de instalação e migração de ambientes, capacitações e os serviços de implementação do ambiente de contingência deverão ser entregues, instalados e estar operacionais, conforme definido abaixo:

2.9.2.1. A solução, com seus componentes, deverá ser entregue, instalada e configurada conforme solicitado no edital, de forma a estarem operacionais em até 60 (sessenta) dias corridos a partir da assinatura do contrato.

## **3.0 Níveis de Serviço**

### **3.1. Suporte técnico à Solução ofertada**

3.1.1. Possuir suporte técnico para a solução, bem como para seus acessórios, durante o período de vigência do contrato, assegurando prazos de atendimento compatíveis com a instalação, ou seja, 24 (vinte e quatro) horas por dia e 7 (sete) dias por semana (à exceção dos chamados de Severidade 4), para um período de 48 (quarenta e oito) meses.

3.1.2. O atendimento aos chamados deverá obedecer a seguinte classificação quanto ao nível de severidade:

<b>Severidade</b>	<b>Descrição</b>	<b>Tipo de Atendimento</b>	<b>Tempo de Atendimento</b>	<b>Tempo de Solução</b>
1 – Crítica	Chamados referentes a situações de emergência ou problema crítico, caracterizados pela existência de ambiente paralisado.	On-site.	No máximo 2 (duas) horas após a abertura do chamado, incluindo percurso do técnico até as instalações do SERPRO.	No máximo 4 (quatro) horas após o início do atendimento do chamado.
2 - Alta	Chamados associados a situações de alto impacto, incluindo os casos de degradação severa de desempenho.	On-site.	No máximo 2 (duas) horas após a abertura do chamado, incluindo percurso do técnico até as instalações do SERPRO.	No máximo 8 (oito) horas após o início do atendimento do chamado.
3 – Média	Chamados referentes a situações de baixo impacto ou para aqueles problemas que	Remoto, com exceção das situações em que seja necessária intervenção	No máximo 4 (quatro) horas após a abertura do chamado.	No máximo 10 (dez) horas após o início do atendimento do chamado.

	se apresentem de forma intermitente, incluindo os casos em que haja necessidade de substituição de componente(s).	física.		
4 – Baixa	Chamados com o objetivo de sanar dúvidas quanto ao uso ou à implementação do produto.	Remoto.	No máximo 24 (vinte e quatro) horas após a abertura do chamado.	No máximo 72 (setenta e duas) horas após a abertura do chamado.

### 3.2. Chamados, Registros e Início de Prazos

3.2.1. Será aberto um chamado para cada problema reportado.

3.2.2. A abertura do chamado na CONTRATADA pelo SERPRO poderá ser realizado através de telefone e/ou WEB.

3.2.3. Os prazos para atendimento de chamados de qualquer severidade serão considerados a partir da hora em que o chamado é aberto, isto é, registrado na CONTRATADA, recebendo dela uma identificação para acompanhamento, controle e histórico.

3.2.4. Será aberto um chamado técnico para cada problema reportado, sendo iniciada a contagem do tempo de atendimento a partir da hora de acionamento.

#### 3.2.5. Tratamento dos chamados de Severidade 1

3.2.5.1. Os chamados de Severidade 1 serão atendidos on-site em no máximo 2 (duas) horas após a sua abertura, incluindo o percurso do técnico até as instalações do SERPRO e contarão com esforço concentrado da contratada com vistas a aplicar solução ou medida de contorno em até 4 (quatro) horas após o início do atendimento do chamado.

3.2.5.2. O atendimento de Severidade 1 não poderá ser interrompido até o completo restabelecimento do produto envolvido, mesmo que se estenda por períodos noturnos e dias não úteis.

#### 3.2.6. Tratamento dos chamados de Severidade 2

3.2.6.1. Os chamados de Severidade 2 serão atendidos on-site em no máximo 2 (duas) horas após a sua abertura, incluindo o percurso do técnico até as instalações do SERPRO e contarão com esforço concentrado da contratada com vistas a aplicar solução ou medida de contorno em até 8 (oito) horas após o início do atendimento do chamado.

3.2.6.2. O atendimento de Severidade 2 não poderá ser interrompido até o completo restabelecimento do produto envolvido, mesmo que se estenda por períodos noturnos e dias não úteis.

3.2.6.3. Os chamados classificados com Severidade 2, quando não solucionados no tempo definido, serão automaticamente escalados para Severidade 1, sendo que os prazos de atendimento e de solução serão automaticamente escalados para o novo nível de severidade.

#### 3.2.7. Tratamento dos chamados de Severidade 3

3.2.7.1. Os chamados de Severidade 3 serão atendidos em no máximo 4 (quatro) horas após a sua abertura e contarão com esforço concentrado da contratada com vistas a aplicar solução ou medida de contorno em até 10 (dez) horas após o início do atendimento do chamado.

3.2.7.2. Caso o problema não possa ser resolvido remotamente, a contratada deverá colocar à disposição do SERPRO, um especialista devidamente habilitado e credenciado que trabalhará o tempo que for necessário para a solução do problema, sendo que o ônus financeiro de tal providência será da contratada.

3.2.7.3. Os chamados classificados com Severidade 3, quando não solucionados no tempo definido, serão automaticamente escalados para Severidade 2, sendo que os prazos de atendimento e de solução serão automaticamente escalados para o novo nível de severidade.

#### **3.2.8. Tratamento dos chamados de Severidade 4**

3.2.8.1. Os chamados de Severidade 4 serão atendidos em no máximo 24 (vinte e quatro) horas após a sua abertura e deverão ser concluídos em até 72 (setenta e duas) horas após a abertura do chamado.

3.2.8.2. Os chamados classificados com Severidade 4 serão atendidos em horário comercial, ou seja, das 08h00min às 18h00min, de segunda-feira a sexta-feira, horário de Brasília.

3.2.9. Por necessidade de serviço, o SERPRO poderá solicitar a escalação de chamado para níveis superiores de severidade. Os prazos dos chamados escalados passam a contar novamente do início.

#### **3.2.10. Manutenções**

3.2.10.1. A CONTRATADA deverá prover, sempre que necessário, todas as correções e/ou atualizações dos hardwares instalados, tais como: nível de firmware e microcódigos, que permitam melhorar as funcionalidades dos equipamentos, bem como mantê-los compatíveis com os demais componentes de hardware e software dos Centros de Dados do SERPRO, sem ônus adicional para o SERPRO.

3.2.10.2. A CONTRATADA deverá realizar manutenção preventiva de acordo com o especificado no Manual do Fabricante do equipamento, tanto do hardware quanto do firmware instalados, sendo de responsabilidade do fornecedor prover todas as correções e/ou atualizações necessárias, de forma sistemática e programada.

3.2.10.3. No caso de manutenções, preventivas ou corretivas, em que haja risco de indisponibilidade total ou parcial dos equipamentos, o SERPRO deverá ser previamente notificado para que se proceda à aprovação e o agendamento da manutenção em horário conveniente ao SERPRO.

3.2.10.4. A CONTRATADA deverá prover suporte remoto pró-ativo e auto-call, via linha telefônica, com monitoração 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, utilizando a infraestrutura existente nas Regionais do SERPRO.

3.2.10.5. Em qualquer hipótese (e ainda que não seja o fabricante dos equipamentos) a CONTRATADA deverá possuir acesso para suporte técnico de 2º e 3º níveis, bem como aos firmwares e microcódigos dos equipamentos, de forma a prestar os serviços de manutenção e assistência técnica, sem ônus adicional para o SERPRO. Para todos os efeitos da contratação em espécie, vigoram os seguintes conceitos:

3.2.10.6. Suporte Técnico Primeiro Nível: equipe treinada para atender diretamente os usuários em demandas referentes a diagnóstico e tratamento de problemas, configuração e administração do ambiente e esclarecimento de dúvidas em geral.

3.2.10.7. Suporte Técnico Segundo Nível: equipe multidisciplinar treinada, certificada e com grande experiência em ambientes críticos e complexos, que exigem alta disponibilidade.

3.2.10.8. Suporte Técnico Terceiro Nível: escalonamento ao fabricante, devido à necessidade de retaguarda nas tecnologias suportadas.

#### **3.2.11. Canais de atendimento**

3.2.11.1. Atendimento através de canal telefônico gratuito 0800, 24 (vinte e quatro) horas por dia, 7(sete) dias por semana.

3.2.11.2. Chamado técnico através de site na Internet, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana e/ou canal telefônico gratuito 0800.

3.2.11.3. Acionamento automático da CONTRATADA no caso de falha de quaisquer dos componentes do(s) equipamento(s) instalado(s).

#### **3.2.12. Escalação de Severidade**

3.2.12.1. Por necessidade de serviço ou criticidade do problema, o SERPRO poderá solicitar a escalação de chamado para níveis superiores ou inferiores de severidade e/ou seus respectivos prazos.

### **3.2.13. Monitoramento do Atendimento dos Chamados**

3.2.13.1. Todos os chamados serão controlados por sistema de informação da CONTRATADA.  
3.2.13.2. Para efeito de acompanhamento das providências e do tempo decorrido desde a sua abertura, o SERPRO será informado sobre cada abertura e fechamento de chamado efetuado por força da presente contratação.

3.2.13.3. O fechamento do chamado poderá se dar quer pela aplicação de correção ao produto ou pela aplicação de solução de contorno que possibilite a operação do sistema.

3.2.13.4. A disponibilização de medida corretiva definitiva poderá, a critério da CONTRATADA, vir a ser incorporada em futuras versões do software.

3.2.13.5. Antes do fechamento de cada chamado a CONTRATADA consultará o SERPRO para validar o fechamento do chamado.

3.2.13.6. Um chamado fechado sem anuência do SERPRO ou sem que o problema tenha sido de fato resolvido, será reaberto e os prazos serão contados a partir da abertura original do chamado, inclusive para efeito de aplicação das sanções previstas.

3.2.13.7. A CONTRATADA manterá cadastro das pessoas indicadas pelo SERPRO que poderão efetuar abertura e autorizar fechamento de chamados.

### **3.2.14. Relatórios sobre a Prestação dos Serviços**

3.2.14.1. A CONTRATADA emitirá relatórios mensais referentes à prestação dos serviços, incluindo informações sintéticas dos chamados abertos e fechados, com ênfase para aqueles resolvidos no mês, informações sobre a disponibilização de novas versões e outras informações consideradas de relevância.

3.2.14.2. A CONTRATADA deve incluir nos relatórios no mínimo as informações do técnico do SERPRO responsável pela abertura do chamado, nível de severidade do chamado, a data e hora da abertura, data e hora do fechamento e solução aplicada.

### **3.2.15. Canais de atendimento**

3.2.15.1. O atendimento será feito por meio do endereço web e/ou através de telefone gratuito 0800, a ser fornecido pela CONTRATADA quando da apresentação da proposta.

3.2.15.2. O atendimento deverá estar disponível 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

### **3.3. Penalidades**

3.3.1. A interrupção do atendimento de um chamado por parte da CONTRATADA, que não tenha sido previamente autorizada pelo SERPRO, ensejará aplicação de multa, conforme o nível de severidade do mesmo:

3.3.2. O não atendimento dentro do prazo estabelecido para o chamado ensejará aplicação de multa à contratada, conforme o nível de severidade do mesmo:

**Severidade 1** – 0,13% (treze décimos por cento) do valor TOTAL da aquisição constante no contrato para o item (equipamento) correspondente, por hora ou fração de hora de atraso.

**Severidade 2** – 0,10% (dez décimos por cento) do valor TOTAL da aquisição constante no contrato para o item (equipamento) correspondente, por hora ou fração de hora de atraso.

**Severidade 3** – 0,05% (cinco centésimos por cento) do valor TOTAL da aquisição constante no contrato para o item (equipamento) correspondente, por hora ou fração de hora de atraso.

**Severidade 4** – 0,03% (três centésimos por cento) do valor TOTAL da aquisição constante no contrato para o item (equipamento) correspondente, por hora ou fração de hora de atraso.

## **4.0 Especificação de Valores e Forma de Pagamento**

Não se aplica

## **5.0 Justificativa da Contratação**

Não se aplica

## **6.0 Seleção do Contratado**

O certame licitatório será através de Pregão Eletrônico, inicialmente pelo menor preço ofertado e

a seleção da contratada dar-se-á nas seguintes condições:

## **6.1. Documentação e Homologação**

6.1.1. A LICITANTE com a proposta de menor preço deverá apresentar em até 5 ( cinco) dias úteis após solicitação do pregoeiro, documentação técnica do fabricante da solução comprovando o atendimento a todos os requisitos contidos na Especificação do objeto a ser contratado, bem como o atendimento das seguintes condições:

6.1.1.1. Documentação técnica do fabricante. Nessa documentação, a LICITANTE deve fornecer uma planilha ponto a ponto indicando documento e página onde consta o cumprimento de cada um dos requisitos das especificações técnicas;

6.1.1.2. Não serão aceitas referências a futuros releases ou versões de produtos para comprovar a existência ou aderência à qualquer quesito desta especificação;

6.1.1.3. Cada documento apresentado deve descrever claramente a referência ao modelo apresentado na proposta, não sendo válidas referências genéricas, e deverão seguir as formas de apresentação definidas na Especificação do Objeto.

6.1.1.4. Será aceita Carta do Fabricante, como comprovação de atendimento de requisitos técnicos e de compatibilidade especificados neste edital, apenas para os itens que não constarem na documentação da maioria dos fabricantes ou que não puderem ser mensurados;

6.1.1.5. Não será aceita Carta do Fornecedor, como comprovação de atendimento à requisitos técnicos e de compatibilidade especificados neste edital;

6.1.1.6. Relação de componentes, incluindo módulos, fontes e acessórios, de cada equipamento que compõe a solução, contendo o código do produto (fabricante) e as respectivas quantidades em cada item;

6.1.1.7. Caso, a documentação apresentada deixe de comprovar o atendimento de um único item da especificação técnica, a proposta será desclassificada, não passando para a etapa seguinte de testes das funcionalidades especificadas.

6.1.1.8. A proposta comercial a ser apresentada pela LICITANTE deverá discriminar os valores de todos os itens que compõem a solução ofertada, incluindo hardware, software e acessórios.

6.1.1.9. Avaliação prática, da EMPRESA LICITANTE CLASSIFICADA E APTA, em bancada de testes de características e funcionalidades exigidas nos itens: ITEM I, ITEM II, ITEM III, ITEM IV, ITEM V e ITEM VI.

6.1.1.9.1. Esta etapa caberá à EMPRESA LICITANTE CLASSIFICADA E APTA, para todos os itens marcados como (AMOSTRA), comprovar na prática, através de testes de bancada, as características e funcionalidades exigidas, onde deverão ser utilizados equipamentos de homologação da EMPRESA LICITANTE CLASSIFICADA E APTA – não incorrendo em encargos ao SERPRO.

6.1.1.9.2. Esta etapa será executada por prepostos do SERPRO em conjunto com os prepostos da EMPRESA LICITANTE CLASSIFICADA E APTA.

6.2. Toda homologação através de (AMOSTRA), deverá ser realizada na dependências do SERPRO de Brasília.

6.3. Somente após a etapa de homologação será definida a EMPRESA LICITANTE VENCEDORA do processo licitatório.

6.3.1. Todos os testes e relacionamento dos técnicos da LICITANTE com o SERPRO deverão ser efetuados no idioma português;

6.3.2. Caso apenas um item referente às especificações seja considerado não atendido, a proposta será totalmente desclassificada;

6.3.3. A LICITANTE deverá indicar previamente os nomes de, no máximo, 6 (seis) técnicos para participação integral durante a realização dos testes de bancada e homologação. Esses técnicos deverão ser representantes legais da LICITANTE, comprovado através documentação de vínculo contratual ou procuração;

6.3.4. A LICITANTE deverá indicar previamente os nomes dos seus técnicos responsáveis pela instalação dos equipamentos nas dependências do SERPRO em número a ser definido pela

proponente.

6.3.5. A critério da LICITANTE, as etapas do aceite poderão ser acompanhados por técnico do fabricante;

6.3.6. Dos técnicos indicados pela LICITANTE, apenas um poderá ser substituído após o início dos testes de bancada, desde que seja comunicado formalmente ao SERPRO;

6.3.7. As empresas concorrentes do pregão poderão indicar técnicos (apenas um para cada empresa) para acompanhar os testes de bancada. As indicações deverão ser realizadas com, no mínimo, 2 dias de antecedência e apenas serão permitidos questionamentos diretos aos técnicos do SERPRO;

6.3.8. No caso de ausência, em qualquer dos períodos durante a realização dos testes de bancada, dos técnicos indicados pelas demais empresas concorrentes do pregão, não serão aceitos quaisquer questionamentos sobre sua realização;

6.3.9. Durante a realização dos testes de bancada serão permitidas quantas forem necessárias, atualizações de software e sistema operacional dos equipamentos sob avaliação, visando a correção ou adaptação para atendimento aos requisitos do edital. Essas atualizações poderão corrigir mais de um item simultaneamente;

6.3.10. A licitação deverá ocorrer em lote único devido à necessidade de compatibilidade técnica entre os itens a serem contratados, o que caso não aconteça, inviabilizará a implantação e o funcionamento da Solução, que por definição da IN-SLTI nº 04, de 19/05/2008, entende-se por todos os serviços, produtos e outros elementos necessários que se integram para o alcance dos resultados pretendidos com a contratação de informática. Ademais, a aquisição em lote único pressupõe contratos de manutenção menos onerosos, economia de recursos da administração, aproveitamento do conhecimento comum das equipes técnicas das regionais em relação ao produto, garantia de compatibilidade e interoperabilidade entre todos os segmentos da rede SERPRO. Por fim, é válido ressaltar a economia gerada em função da redução de custos consequente da agregação dos quantitativos de hardware, software e serviços de TIC a serem fornecidos, em relação à oferta;

6.3.11. Os serviços de instalação e o repasse de conhecimento especializada também deverão compor o objeto único, uma vez que não se pode especificar previamente qual solução será contratada, enquanto diversos fornecedores apresentam soluções específicas e de diferentes modelos de implementação. Essa alternativa desenvolveu-se a partir da constatação comum, reiteradamente experimentada, da inviabilidade da obtenção de resultados satisfatórios por meio de fornecedores autônomos diversos. Mais uma vez, a ressalva sobre a redução de custos, consequente da aquisição integrada, faz-se válida para tais serviços.

6.3.12. Os testes deverão ser realizados no horário compreendido entre 09:00 h e 17:00 h de segunda à sexta-feira.

6.3.13. A modalidade para realização da aquisição será pregão eletrônico e a adjudicação será pelo menor valor global.

#### **6.4. Homologação da Solução**

6.4.1. Após aceite da documentação comprobatória, a LICITANTE deverá disponibilizar para a realização das etapas de homologação, no prazo de até 30 (trinta) dias corridos contados à partir da solicitação do pregoeiro, amostra da mesma marca e modelo ofertado na proposta, conforme especificação do objeto;

6.4.2. A LICITANTE deverá disponibilizar adicionalmente todos os demais equipamentos necessários para a realização dos testes de bancada;

6.4.3. O SERPRO fornecerá um prazo de 10 (dez) dias úteis para a realização da fase de homologação.

6.4.4. O prazo de homologação poderá ser prorrogado por igual período a critério do SERPRO.

#### **7.0 Justificativa para Aceitação de Preços**

Não se aplica

## **8.0 Gerenciamento do Contrato**

### **8.1. Obrigações da Contratada**

#### **8.1.1. Repasse de Conhecimento**

8.1.1. Como parte integrante do processo de instalação, configuração, implantação, implementação e produção, a empresa vencedora deverá realizar o repasse de conhecimento para o SERPRO, dos conhecimentos necessários para instalar, administrar, configurar, operar, desenvolver e gerenciar os produtos fornecidos, conforme descrito a seguir:

8.1.1.1. As capacitações tecnológicas terão conteúdo e carga horária em consonância com os cursos oficiais do fabricante da solução, vigentes à época da sua realização.

8.1.1.2. O repasse de conhecimento para o SERPRO deverá ser iniciado em até 30 (trinta) dias após o aceite da solução, podendo ser adiada por conveniência do SERPRO, quando então, em comum acordo com a CONTRATADA, será marcada a data definitiva;

8.1.1.3. A licitante vencedora deverá entregar o Conteúdo programático de todos os treinamentos, para aprovação pelo SERPRO;

8.1.1.4. A empresa vencedora deverá fornecer, a cada ano de vigência do contrato, o repasse de conhecimento para o SERPRO em 02 (duas) localidades a serem definidas pelo SERPRO, para até 15 (quinze) pessoas por localidade, abrangendo: administração, configuração básica e avançada, gerenciamento, desenvolvimento e novas funcionalidades. O conteúdo poderá ser redefinido de acordo com as necessidades do SERPRO;

8.1.1.5. A data de início destas capacitações adicionais e o local de realização serão definidos pelo SERPRO de acordo com suas necessidades. O SERPRO deverá comunicar formalmente o fornecedor com uma antecedência mínima de 60 (sessenta) dias;

8.1.1.6. A capacitação deverá possuir carga horária mínima de 40 (quarenta) horas e deverá ocorrer em período integral.

8.1.1.7. A capacitação deverá ser ministrada por profissional(ais) certificado(s) e/ou autorizado(s) pelo fabricante da(s) solução(ões);

8.1.1.8. A contratada deverá apresentar com antecedência de, no mínimo, 10 (dez) dias do início da capacitação, os certificado(s) solicitado(s) bem como declaração de que a empresa está autorizada pelo fabricante a prestar a capacitação;

8.1.1.9. O material da capacitação deve ser original e de boa qualidade e aprovado pelo SERPRO;

8.1.1.10. Todas as despesas com material, equipamentos, instrutores, deslocamento de instrutores e demais itens serão de responsabilidade do fornecedor;

8.1.1.11. Após cada capacitação deverá ser emitido certificado para cada participante, obedecendo aos critérios de frequência previamente negociados com o SERPRO;

8.1.2. O não atendimento a um dos itens e subitens descritos em repasse de conhecimento para o SERPRO ensejará aplicação de multa à CONTRATADA no valor equivalente a 1,0% (um por cento) do valor do contrato, por hora ou fração de hora de atraso, limitado a 20% (vinte por cento) do valor total do contrato;

8.1.3. Os custos de deslocamento dos profissionais do SERPRO selecionados para o repasse de conhecimento para o SERPRO, quando existirem, será de responsabilidade do SERPRO;

8.1.4. Deverão ser disponibilizadas, por meio de convite oficial, no mínimo, 2 (duas) vagas para participação em eventos ou similares para atualização tecnológica, no Brasil ou no exterior, além do curso de capacitação indicado nesta seção.

8.1.5. A CONTRATADA deverá prover toda a logística e todo o material necessário à execução do repasse de conhecimento teórico e prático, ou seja, instalações adequadas, equipamentos, manuais e apostilas didáticas. Os manuais e apostilas fornecidos devem ser originais e oficiais do fabricante;

8.1.6. O repasse de conhecimento deverá ser realizado utilizando conteúdo teórico e prático, através de laboratório preparado com equipamentos equivalentes aos ofertados, onde estarão disponíveis as mesmas funcionalidades solicitadas nas especificações técnicas dos itens;

8.1.7. O repasse de conhecimento para o SERPRO deverá ser realizado de acordo com o perfil



de atuação, tendo como base o Perfil de Administrador: Após o repasse de conhecimento os empregados deverão estar aptos a Administrar, Configurar, Operar e Gerenciar a solução contratada.

8.1.8. Para atendimento ao item 8.1.7. serão realizadas capacitações para três turmas de 12 (doze) pessoas, 1 (uma) em Brasília-DF, 1(uma) em São Paulo e 1(uma) em Recife, sem ônus para o SERPRO, fornecendo a infraestrutura necessária (no mínimo 1 estação para cada 2 participantes), a ser realizada após a homologação e aceite da solução;

8.1.9. O número total de turmas e o número máximo de alunos por turma previstos no item 8.1.8. poderá ser modificado em comum acordo desde que sejam mantidos o número de funcionários capacitados.

## **8.2. Operação Assistida**

8.2.1. A Contratada deve prover durante o primeiro ano da garantia, operação assistida para todos os elementos que compõem a solução ofertada, iniciando-se à partir da entrega da solução em produção plena e após o aceite final (definitivo).

8.2.2. A Contratada deve prover a operação assistida localmente, na unidade de Brasília.

8.2.3. A operação assistida deve ser provida em modelo 8x5 (horário comercial e dias úteis). Com a presença física de no mínimo um técnico.

8.2.4. A Contratada deverá prover relatório mensal ao SERPRO informando as ações tomadas durante este período.

8.2.5. O escopo da operação assistida consiste no suporte à equipe de Operação e Manutenção do SERPRO, provendo esta equipe com sugestões de melhores práticas e configurações da solução.

8.2.6. Em caso de necessidade de deslocamento do técnico para o ambiente do SERPRO, este ocorrerá por conta da Contratada.

## **9.0 Considerações Gerais**

9.1. A empresa Licitante deverá apresentar documento(s) que comprove(m) a aptidão técnica necessária para executar o objeto, tais como contrato, termo, certificado, declaração, endereço eletrônico de sítios oficiais do fabricante na internet, entre outros documentos pertinentes que demonstrem de forma inequívoca, a habilidade técnica para prestar o serviço de suporte técnico e vínculo vigente com o fabricante do hardware e/ou do software.

9.2. Não haverá necessidade de apresentação da declaração prevista no item 9.1, quando a licitante for a própria fabricante do hardware e/ou software.

## **Elaboração**

Data : 10/04/2012

EDUARDO LIMA - 12005240

COGTI/CIPOA