

CONTRATO Nº 77/2016

**CONTRATO Nº 77/2016 QUE ENTRE SI
CELEBRAM O ESTADO DO PIAUÍ POR
INTERMÉDIO DA PROCURADORIA-
GERAL DE JUSTIÇA E A EMPRESA
APPROACH TECNOLOGIA LTDA.
PROCESSO ADMINISTRATIVO Nº
27.090/2016.**

CONTRATANTE: O Estado do Piauí, pessoa jurídica de direito público, por intermédio da Procuradoria-Geral de Justiça, com sede na Rua Álvaro Mendes, nº 2294, Centro, Teresina-PI, inscrito no CNPJ: 05.805.924/0001-89, representado neste ato pela Procuradora-Geral de Justiça em exercício, Zélia Saraiva Lima, no uso da competência que lhe é atribuída pelo art. 12, V, da Lei Complementar Estadual Nº 12, de 18 de dezembro de 1993.

CONTRATADO: EMPRESA APPROACH TECNOLOGIA LTDA, inscrita no CNPJ sob o nº 24.376.542/0001-21 estabelecido na Avenida Prefeito Osmar Cunha, nº 416, Sala nº 505, Centro, Florianópolis-SC, CEP: 88.015-100 representado pelo Sr. Kent Johann Modes, portador da Carteira de Identidade nº 4826448 SSP/SC e CPF nº 478.629- de acordo com a representação legal que lhe é outorgada por instrumento público (fl. 85).

Os CONTRATANTES têm entre si, justo e avençado, e celebram o presente instrumento, instruído no Contrato n.º 77/2016 (Adesão n.º 22/2016), Processo Administrativo nº 27.090/2016, mediante as cláusulas e condições que se seguem:

CLÁUSULA PRIMEIRA - DO PROCEDIMENTO

1.1 O presente Contrato obedece aos termos da Adesão nº 22/2016, a Ata de Registro de Preços nº 128/2016 da Universidade Federal do Amapá - UNIFAP, a proposta de preços apresentada pela contratada, às disposições da Lei nº 10.520/02, nº 8.666/93 e do Decreto Estadual nº 11.319/04.

CLÁUSULA SEGUNDA - DO OBJETO

2.1 Aquisição de Firewall para prover proteção aos servidores, estação de trabalho e demais dispositivos conectados à rede com conexões originadas ou destinadas à internet do MP/PI.

ITEM	QTD	DESCRIÇÃO	VALOR UNITÁRIO	VALOR TOTAL
1	2	FIREWALL TIPO 1 com instalação/configuração	R\$185.000,00	R\$370.000,00

ORDEM	CONFIGURAÇÃO MÍNIMA
1.1	<p>DESCRIÇÃO</p> <p>a) Aquisição de Solução de proteção de rede com características de Next Generation Firewall (NGFW) para segurança de informação perimetral que inclui filtro de pacote, controle de aplicação, administração de largura de banda (QoS), VPN IPSec e SSL, IPS, prevenção contra ameaças de vírus, spywares e malwares "Zero Day", Filtro de URL, bem como controle de transmissão de dados e acesso a internet compondo uma plataforma de segurança integrada e robusta;</p> <p>b) Por plataforma de segurança entende-se hardware e software integrados do tipo appliance;</p> <p>c) O equipamento ofertado deve ser gerenciado pelo software de gerenciamento marca Palo Alto, modelo Panorama, já existente no MP/PI e compatível com as seguintes funcionalidades;</p> <ul style="list-style-type: none"> ✓ Possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos de firewall; ✓ Permitir controle global de políticas para todos os equipamentos que compõe a plataforma de segurança, os já existentes e também os que serão ofertados neste item; ✓ Exportar backup de configuração automaticamente via agendamento;
1.2	<p>CAPACIDADES E QUANTIDADES</p> <p>a) Throughput de 2 Gbps com a funcionalidade de controle de aplicação habilitada para todas as assinaturas que o fabricante possuir;</p> <p>b) Throughput de 1 Gbps com as seguintes funcionalidade habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação IPS, Antivírus e Antispyware. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito;</p> <p>c) Os throughputs devem ser comprovados por documento de domínio público do fabricante. A ausência de tais documentos comprobatórios</p>

(Handwritten signature and mark)

	<p>reservará ao órgão o direito de aferir a performance dos equipamentos em bancada, assim como atendimento de todas as funcionalidades especificadas neste edital. Caso seja comprovado o não atendimento das especificações mínimas nos testes de bancada, serão considerados inabilitados e sujeitos as sanções previstas em lei;</p> <p>d) Não será aceito a comprovação de Throughput para funcionalidades de camada 7 (Controle de Aplicação e IPS, por exemplo), com tráfego UDP e/ou RFCs baseadas neste protocolo;</p> <p>e) Quando as funcionalidades de controle de aplicação, IPS, antivírus e anti-spyware tiverem habilitadas de forma simultânea o tráfego deverá ser inspecionado de modo bidirecional com inspeção em toda a sessão do pacote, sem qualquer utilização de recurso de by-pass. Não será aceito aceleração de pacotes na placa de rede limitando a análise somente até camada 4;</p> <p>f) Suporte a, no mínimo, 240.000 conexões simultâneas;</p> <p>g) Suporte a, no mínimo, 45.000 novas conexões por segundo;</p> <p>h) Fonte 120/240 AC;</p> <p>i) Disco Solid State Drive (SSD) de, no mínimo, 100 GB;</p> <p>j) Deve possuir, no mínimo, 10 (dez) interfaces de rede 10/100/1000 base-TX;</p> <p>k) Deve possuir, no mínimo, 06 (seis) interfaces de rede 01 Gbps SFP;</p> <p>l) Deve possuir, no mínimo, 02 (duas) Gbps interfaces dedicadas para alta disponibilidade;</p> <p>m) Deve possuir, no mínimo, 01 (uma) interface de rede 01 Gbps dedicada para gerenciamento;</p> <p>n) Deve possuir, no mínimo, 01 (uma) interface do tipo console ou similar;</p> <p>o) Suporte a, no mínimo, 10 (dez) roteadores virtuais;</p> <p>p) Suporte a, no mínimo, 30 (trinta) zonas de segurança;</p> <p>q) Estar licenciada para ou suportar sem o uso de licença, 1000 (mil) clientes de VPN SSL simultâneos;</p> <p>r) Estar licenciada para ou suportar sem o uso de licença, 1000 (mil) túneis de VPN IPSEC simultâneos;</p>
1.3	<p>CARACTERISTICAS GERAIS</p> <p>a) Por cada equipamento que compõe a plataforma de segurança, entende-se o hardware e as licenças de softwares necessárias para o seu funcionamento;</p> <p>b) Por console de gerência e monitoração, entende-se as licenças de software necessárias para as duas funcionalidades, bem como hardware dedicado para o funcionamento das mesmas;</p> <p>c) A console de gerência e monitoração podem residir no mesmo appliance de proteção de rede, desde que possuam recurso de CPU, memória, interface de rede e sistema operacional dedicados para esta função;</p> <p>d) Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale</p> <p>e) A solução deve consistir de appliance de proteção de rede com funcionalidades de Next Generation Firewall (NGFW), e console de gerência e monitoração;</p>



- f) Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;
- g) As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação;
- h) A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;
- i) O hardware e software que executem as funcionalidades de proteção de rede, bem como a console de gerência e monitoração, devem ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;
- j) Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19", incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;**
- k) O software deverá ser fornecido em sua versão mais atualizada;
- l) Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:**
- l.1) Suporte a 4094 VLAN Tags 802.1q;
 - l.2) Agregação de links 802.3ad e LACP;
 - l.3) Policy based routing ou policy based forwarding;
 - l.4) Roteamento multicast (PIM-SM);
 - l.5) DHCP Relay;
 - l.6) DHCP Server;
 - l.7) Jumbo Frames;
 - l.8) Suporte a criação de objetos de rede que possam ser utilizados como endereço IP de interfaces L3;
- m) Suportar sub-interfaces ethernet logicas;
- n) Deve suportar os seguintes tipos de NAT:**
- n.1) Nat dinâmico (Many-to-1);
 - n.2) Nat dinâmico (Many-to-Many);
 - n.3) Nat estático (1-to-1);
 - n.4) NAT estático (Many-to-Many);
 - n.5) Nat estático bidirecional 1-to-1;
 - n.6) Tradução de porta (PAT);
 - n.7) NAT de Origem;
 - n.8) NAT de Destino;
 - n.9) Suportar NAT de Origem e NAT de Destino simultaneamente;
- o) Deve implementar Network Prefix Translation (NPTv6), prevenindo problemas de roteamento assimétrico;
- p) Deve implementar o protocolo ECMP;**
- q) Deve implementar balanceamento de link por hash do IP de origem;**
- r) Deve implementar balanceamento de link por hash do IP de origem e destino;**
- s) Deve implementar balanceamento de link através do método round-robin;
- t) Deve implementar balanceamento de link por peso. Nesta opção deve ser



possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, quatro links;

u) Deve implementar balanceamento de link através de políticas por usuário e grupos de usuários do LDAP/AD;

v) Deve implementar balanceamento de link através de políticas por aplicação e porta de destino;

w) Deve implementar o protocolo Link Layer Discovery (LLDP), permitindo que o appliance e outros ativos da rede se comuniquem para identificação da topologia da rede em que estão conectados e a função dos mesmos facilitando o processo de troubleshooting. As informações aprendidas e armazenadas pelo appliance devem ser acessíveis via SNMP;

x) Enviar log para sistemas de monitoração externos, simultaneamente;

y) Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;

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

aa) Proteção contra anti-spoofing;

bb) Deve permitir bloquear sessões TCP que usem variações do 3-way hand-shake, como 4 way e 5 way split hand-shake, prevenindo desta forma possíveis tráfegos maliciosos;

cc) Deve exibir nos logs de tráfego o motivo para o término da sessão no firewall, incluindo sessões finalizadas onde houver de-criptografia de SSL e SSH;

dd) Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);

ee) Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);

ff) Suportar a OSPF graceful restart;

gg) Suportar no mínimo as seguintes funcionalidades em IPv6: SLAAC (address auto configuration), NAT64, Identificação de usuários a partir do LDAP/AD, Captive Portal, IPv6 over IPv4 IPSec, Regras de proteção contra DoS (Denial of Service), De-criptografia SSL e SSH, PBF (Policy Based Forwarding), QoS, DHCPv6 Relay, IPSEC, Ativo/Ativo, Ativo/Passivo, SNMP, NTP, SYSLOG, DNS e controle de aplicação;

hh) Dispositivos de proteção devem ter a capacidade de operar de forma simultânea em uma única instância de firewall, mediante o uso de suas interfaces físicas nos seguintes modos: Modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3):

hh.1) Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;

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

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

hh.4) Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;

ii) Suporte a configuração de alta disponibilidade Ativo/Passivo e



	<p>Ativo/Ativo: ii.1) Em modo transparente; / Em layer 3; jj) A configuração em alta disponibilidade deve sincronizar: jj.1) Sessões; jj.2) Configurações, incluindo, mas não limitado a políticas de Firewall, NAT, QOS e objetos de rede; jj.3) Certificados de-criptografados; jj.4) Associações de Segurança das VPNs; jj.5) Tabelas FIB; jj.6) HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link; kk) As funcionalidades de controle de aplicações, VPN IPSec e SSL, QOS, SSL e SSH Decryption e protocolos de roteamento dinâmico devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante;</p>
<p>1.4</p>	<p>CONTROLE POR POLITICA DE FIREWALL a) Deverá suportar controles por zona de segurança; b) Controles de políticas por porta e protocolo; c) Controle de políticas por aplicações grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações; d) Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança; e) Deve suportar a consulta a fontes externas de endereços IP, domínios e URLs podendo ser adicionados nas políticas de firewall para bloqueio ou permissão do tráfego; f) Controle de políticas por código de País (Por exemplo: BR, USA, UK, RUS); g) Controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound); h) Deve suportar offload de certificado em inspeção de conexões SSL de entrada (Inbound); i) Deve de-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.2; j) Controle de inspeção e de-criptografia de SSH por política; k) A política de criptografia de SSH deve possibilitar a identificação e bloqueio de tráfego caso o protocolo esteja sendo usado para tunelar aplicações como técnica evasiva para burlar os controles de segurança; l) A plataforma de segurança deve implementar espelhamento de tráfego de-criptografado (SSL e TLS) para soluções externas de análise (Forense de rede, DLP, Análise de Ameaças, entre outras); m) É permitido uso de appliance externo, específico para a de-criptografia de (SSL e TLS), com espelhamento de cópia do tráfego de-criptografado tanto para o firewall, quanto para as soluções de análise. n) Bloqueios dos seguintes tipos de arquivos: bat, cab, dll, exe, pif, e reg</p>

[Handwritten signature]

	<p>o) Traffic shaping QoS baseado em Políticas (Prioridade, Garantia e Máximo)</p> <p>p) QoS baseado em políticas para marcação de pacotes (diffserv marking), inclusive por aplicações.</p> <p>q) Suporte a objetos e regras IPV6.</p> <p>r) Suporte a objetos e regras multicast.</p> <p>s) Deve suportar no mínimo três tipos de negação de tráfego nas políticas de firewall: Drop sem notificação do bloqueio ao usuário, Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego, TCP-Reset para o client, TCP-Reset para o server ou para os dois lados da conexão;</p> <p>t) Suportar a atribuição de agendamento as políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;</p>
<p>1.5</p>	<p>CONTROLE DE APLICAÇÕES</p> <p>a) Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos.</p> <p>b) Reconhecer pelo menos 1700 aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;</p> <p>c) Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs, etc;</p> <p>d) Deve inspecionar o payload de pacote de dados com o objetivo de detectar através de expressões regulares assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo. A checagem de assinaturas também deve determinar se uma aplicação está utilizando a porta default ou não, incluindo, mas não limitado a RDP na porta 80 ao invés de 389;</p> <p>e) Deve aplicar heurística a fim de detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a Encrypted Bittorrent e aplicações VOIP que utilizam criptografia proprietária;</p> <p>f) Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e ataques mediante a porta 443.</p> <p>g) Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;</p> <p>h) Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado a Yahoo Instant Messenger usando HTTP. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação,</p>



incluindo, mas não limitado a compartilhamento de arquivo dentro do Webex. Além de detectar arquivos e outros conteúdos que devem ser inspecionados de acordo as regras de segurança implementadas;

i) Deve permitir a utilização de aplicativos para um determinado grupo de usuário e bloquear para o restante, incluindo, mas não limitado a Skype. Deve permitir também a criação de políticas de exceção concedendo o acesso a aplicativos como Skype apenas para alguns usuários;

j) Identificar o uso de táticas evasivas via comunicações criptografadas;

k) Atualizar a base de assinaturas de aplicações automaticamente;

l) Reconhecer aplicações em IPv6;

m) Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos do LDAP/AD;

n) Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;

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

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

q) Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;

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

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

t) fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;

u) Deve alertar o usuário quando uma aplicação for bloqueada;

v) Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;

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

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

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

z) Deve possibilitar a diferenciação de aplicações Proxies (ghostsurf, freegate,



	<p>etc.) possuindo granularidade de controle/políticas para os mesmos;</p> <p>aa) Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como:</p> <p>aa.1) Tecnologia utilizada na aplicações (Client-Server, Browse Based, Network Protocol, etc).</p> <p>aa.2) Nível de risco da aplicação.</p> <p>aa.3) Categoria e sub-categoria de aplicações.</p> <p>aa.4) Aplicações que usem técnicas evasivas, utilizadas por malwares, como transferência de arquivos e/ou uso excessivo de banda, etc;</p>
1.6	<p>PREVENÇÃO DE AMEAÇAS</p> <p>a) Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de Firewall ou entregue através de composição com outro equipamento ou fabricante;</p> <p>b) Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);</p> <p>c) As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante;</p> <p>d) Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;</p> <p>e) Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS, Antipyware e Antivirus: permitir, permitir e gerar log, bloquear, bloquear IP do atacante por um intervalo de tempo e enviar tcp-reset;</p> <p>f) As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;</p> <p>g) Exceções por IP de origem ou de destino devem ser possíveis nas regras, de forma geral e assinatura a assinatura;</p> <p>h) Deve suportar granularidade nas políticas de IPS Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens.</p> <p>i) Deve permitir o bloqueio de vulnerabilidades.</p> <p>j) Deve permitir o bloqueio de exploits conhecidos.</p> <p>k) Deve incluir proteção contra ataques de negação de serviços.</p> <p>l) Deverá possuir os seguintes mecanismos de inspeção de IPS:</p> <p>l.1) Análise de padrões de estado de conexões;</p> <p>l.2) Análise de decodificação de protocolo;</p> <p>l.3) Análise para detecção de anomalias de protocolo;</p> <p>l.4) Análise heurística;</p> <p>l.5) IP Defragmentation;</p> <p>l.6) Remontagem de pacotes de TCP;</p> <p>l.7) Bloqueio de pacotes malformados;</p> <p>m) Ser imune e capaz de impedir ataques básicos como: Synflood, ICMPflood,</p>



UDPflood, etc;

n) Detectar e bloquear a origem de portscans;

o) Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;

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

q) Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;

r) Possuir assinaturas para bloqueio de ataques de buffer overflow;

s) Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;

t) Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS e anti-spyware, permitindo a criação de exceções com granularidade nas configurações;

u) Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;

v) É permitido uso de appliance externo (antivírus de rede), para o bloqueio de vírus e spywares em protocolo SMB de forma a conter malwares se espalhando horizontalmente pela rede;

w) Suportar bloqueio de arquivos por tipo;

x) Identificar e bloquear comunicação com botnets;

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

z) Deve suportar referencia cruzada com CVE;

aa) Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:

bb) O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;

cc) Deve suportar a captura de pacotes (PCAP), por assinatura de IPS e Antispyware;

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

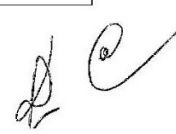
ee) Deve possuir a função resolução de endereços via DNS, para que conexões com destino a domínios maliciosos sejam resolvidas pelo Firewall com endereços (IPv4 e IPv6), previamente definidos;

ff) Permitir o bloqueio de vírus, pelo menos, nos seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;

gg) Os eventos devem identificar o país de onde partiu a ameaça;

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

ii) Proteção contra downloads involuntários usando HTTP de arquivos executáveis.



	<p>jj) Rastreamento de vírus em pdf.</p> <p>kk) Deve permitir a inspeção em arquivos comprimidos que utilizam o algoritmo deflate (zip, gzip, etc.)</p> <p>ll) Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.</p>
1.7	<p>ANALISE DE MALWARE MODERNO</p> <p>a) Devido aos Malwares hoje em dia serem muito dinâmicos e um antivírus comum reativo não ser capaz de detectar os mesmos com a mesma velocidade que suas variações são criadas, a solução ofertada deve possuir funcionalidades para análise de Malwares não conhecidos incluídas na própria ferramenta ou entregue com composição com outro fabricante;</p> <p>b) O dispositivo de proteção deve ser capaz de enviar arquivos trafegados de forma automática para análise "In Cloud" ou local, onde o arquivo será executado e simulado em ambiente controlado;</p> <p>c) Selecionar através de políticas granulares quais tipos de arquivos sofrerão esta análise incluindo, mas não limitado a: endereço IP de origem/destino, usuário/grupo do AD/LDAP, aplicação, porta, URL/categoria de URL de destino, tipo de arquivo e todas estas opções simultaneamente;</p> <p>d) Deve possuir a capacidade de diferenciar arquivos analisados em pelo menos três categorias: malicioso, não malicioso e arquivos não maliciosos, mas com características indesejáveis como softwares que deixa o sistema operacional lento, que alteram parâmetros do sistema, etc.;</p> <p>e) Suportar a análise com pelo menos 100 (cem) tipos de comportamentos maliciosos para a análise da ameaça não conhecida;</p> <p>f) Suportar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows XP, Windows 7 (32 bits) e Windows 7 (64 bits);</p> <p>g) Deve suportar a monitoração de arquivos trafegados na internet (HTTPs, FTP, HTTP, SMTP) como também arquivos trafegados internamente entre servidores de arquivos usando SMB em todos os modos de implementação: sniffer, transparente e L3;</p> <p>h) A solução deve possuir a capacidade de analisar em sand-box links (http e https) presentes no corpo de e-mails trafegados em SMTP e POP3. Deve ser gerado um relatório caso a abertura do link pela sand-box o identifique como site hospedeiro de exploits;</p> <p>i) Para ameaças trafegadas em protocolo SMTP e POP3, a solução deve ter a capacidade de mostrar nos relatórios o remetente, destinatário e assunto dos e-mails permitindo identificação ágil do usuário vítima do ataque;</p> <p>j) O sistema de análise "In Cloud" ou local deve prover informações sobre as ações do Malware na máquina infectada, informações sobre quais aplicações são utilizadas para causar/propagar a infecção, detectar aplicações não</p>



	<p>confiáveis utilizadas pelo Malware, gerar assinaturas de Antivírus e Anti-spyware automaticamente, definir URLs não confiáveis utilizadas pelo novo Malware e prover informações sobre o usuário infectado (seu endereço ip e seu login de rede);</p> <p>k) O sistema automático de análise "In Cloud" ou local deve emitir relatório com identificação de quais soluções de antivírus existentes no mercado possuem assinaturas para bloquear o malware;</p> <p>l) Deve permitir exportar o resultado das análises de malwares de dia Zero em PDF e CSV a partir da própria interface de gerência;</p> <p>m) Deve permitir o download dos malwares identificados a partir da própria interface de gerência;</p> <p>n) Deve permitir visualizar o resultado das análises de malwares de dia zero nos diferentes sistemas operacionais suportados;</p> <p>o) Deve permitir informar ao fabricante quanto a suspeita de ocorrências de falso-positivo e falso-negativo na análise de malwares de dia Zero a partir da própria interface de gerência.</p> <p>p) Caso a solução seja fornecida em appliance local, deve possuir, no mínimo, 28 ambientes controlados (sand-box) independentes para execução simultânea de arquivos suspeitos;</p> <p>q) Caso seja necessário licenças de sistemas operacional e softwares para execução de arquivos no ambiente controlado (sand-box), as mesmas devem ser fornecidas em sua totalidade, sem custos adicionais para a contratante;</p> <p>r) Suportar a análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL no ambiente controlado;</p>
<p>1.8</p>	<p>FILTRO URL</p> <p>a) Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);</p> <p>b) Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, Ips, Redes e Zonas de segurança.</p> <p>c) Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via ldap, Active Directory, E-directory e base de dados local.</p> <p>d) Permite popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório;</p> <p>e) Suporta a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;</p> <p>f) Deve bloquear o acesso a sites de busca (Google, Bing e Yahoo), caso a opção Safe Search esteja desabilitada. Deve ainda exibir página de bloqueio fornecendo instruções ao usuário de como habilitar a função;</p> <p>g) Suporta base ou cache de URLs local no appliance, evitando delay de comunicação/validação das URLs;</p> <p>h) Possui pelo menos 60 categorias de URLs;</p> <p>i) A categorização de URL deve analisar toda a URL e não somente até o nível de diretório;</p>



	<p>j) Suporta a criação categorias de URLs customizadas; k) Suporta a exclusão de URLs do bloqueio, por categoria; l) Permite a customização de página de bloqueio; m) Permite o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão "Continuar" para permitir o usuário continuar acessando o site); n) A funcionalidade de Filtro de URL deve operar em caráter permanente, para base ou cache instalado na solução até a data de vencimento da licença, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante; o) Suporta a inclusão nos logs do produto de informações das atividades dos usuários; p) Deve salvar nos logs as informações dos seguintes campos do cabeçalho HTTP nos acessos a URLs: UserAgent, Referer, e X-Forwarded For;</p>
1.9	<p>IDENTIFICAÇÃO DE USUÁRIOS a) Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via ldap, Active Directory, E-directory e base de dados local; b) Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários; c) Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários; d) Deve implementar a criação de políticas de segurança baseada em atributos específicos do Radius, incluindo mas não limitado a: baseado no sistema operacional do usuário remoto exigir autenticação padrão Windows e on-time password (OTP) para usuários Android; e) Deve possuir integração com Ldap para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários; f) Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via syslog, para a identificação de endereços IP e usuários; g) Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal); h) Suporte a autenticação Kerberos; i) Deve suportar autenticação via Kerberos para administradores da plataforma de segurança, captive Portal e usuário de VPN SSL; j) Deve possuir suporte a identificação de múltiplos usuários conectados em</p>

[Handwritten signature]

	<p>um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;</p> <p>k) Deve identificar usuários através de leitura do campo x-forwarded-for, populando nos logs do firewall o endereço IP, bem como o usuário de rede responsável pelo acesso;</p> <p>l) Deve permitir a criação de políticas de segurança baseadas em usuários de rede com reconhecimento dos mesmos através de leitura do campo x-forwarded-for;</p> <p>m) Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;</p> <p>n) Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em servidores acessados remotamente, mesmo que não sejam servidores Windows;</p>
1.10	<p>QoS</p> <p>a) Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, ustream, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming.</p> <p>b) Suportar a criação de políticas de QoS por:</p> <p>b.1) Endereço de origem;</p> <p>b.2) Endereço de destino;</p> <p>b.3) Por usuário e grupo do LDAP/AD;</p> <p>b.4) Por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;</p> <p>b.5) Por porta;</p> <p>c) QoS deve possibilitar a definição de classes por:</p> <p>c.1) Banda Garantida; / Banda Máxima; / Fila de Prioridade.</p> <p>d) Suportar priorização RealTime de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype.</p> <p>e) Suportar marcação de pacotes Diffserv, inclusive por aplicação;</p> <p>f) Deve implementar QoS (traffic-shapping), para pacotes marcados por outros ativos na rede (DSCP). A priorização e limitação do tráfego deve ser efetuada nos dois sentidos da conexão (inbound e outbound);</p> <p>g) Disponibilizar estatísticas RealTime para classes de QoS.</p> <p>h) Deve suportar QoS (traffic-shapping), em interface agregadas;</p> <p>i) Deverá permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário;</p>
1.11	<p>FILTRO DE DADOS</p> <p>a) Permite a criação de filtros para arquivos e dados pré-definidos;</p> <p>b) Os arquivos devem ser identificados por extensão e assinaturas;</p> <p>c) Permite identificar e opcionalmente prevenir a transferência de vários</p>



	<p>tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (P2P, InstantMessaging, SMB, etc);</p> <p>d) Suportar identificação de arquivos compactados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;</p> <p>e) Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular;</p> <p>f) Permitir listar o número de aplicações suportadas para controle de dados;</p> <p>g) Permitir listar o número de tipos de arquivos suportados para controle de dados;</p>
1.12	<p>GEO LOCALIZAÇÃO</p> <p>a) Suportar a criação de políticas por Geo Localização, permitindo o tráfego de determinado País/Países sejam bloqueados;</p> <p>b) Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos.</p> <p>c) Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas.</p>
1.13	<p>VPN</p> <p>a) Suportar VPN Site-to-Site e Cliente-To-Site;</p> <p>b) Suportar IPSec VPN;</p> <p>c) Suportar SSL VPN;</p> <p>d) A VPN IPSec deve suportar:</p> <p>d.1) DES e 3DES;</p> <p>d.2) Autenticação MD5 e SHA-1;</p> <p>d.3) Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;</p> <p>d.4) Algoritmo Internet Key Exchange (IKEv1 e v2);</p> <p>d.5) AES 128, 192 e 256 (Advanced Encryption Standard)</p> <p>d.6) Autenticação via certificado IKE PKI;</p> <p>e) Deve possuir interoperabilidade com os seguintes fabricantes:</p> <p>e.1) Cisco; / Checkpoint; / Juniper; / Palo Alto Networks; / Fortinet; / Sonic Wall;</p> <p>f) Deve permitir habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de troubleshooting;</p> <p>g) A VPN SSL deve suportar:</p> <p>g.1) usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;</p> <p>g.2) A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;</p> <p>g.3) Atribuição de endereço IP nos clientes remotos de VPN SSL;</p> <p>g.4) Deve permitir a atribuição de IPs fixos nos usuários remotos de VPN SSL;</p>

[Handwritten signature]

- g.5)** Deve permitir a criação de rotas de acesso e faixas de endereços IP atribuídas a clientes remotos de VPN de forma customizada por usuário AD/LDAP e grupo de usuário AD/LDAP;
- g.6)** Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;
- g.7)** Atribuição de DNS nos clientes remotos de VPN;
- g.8)** Deve permitir que seja definido métodos de autenticação distintos por sistema operacional do dispositivo remoto de VPN (Android, IOS, Mac, Windows e Chrome OS);
- g.9)** A solução de VPN deve verificar se o client que está conectando é o mesmo para o qual o certificado foi emitido inicialmente. O acesso deve ser bloqueado caso o dispositivo não seja o correto;
- g.10)** Deve possuir lista de bloqueio para dispositivos que forem reportados com roubado ou perdido pelo usuário;
- g.11)** Deve haver a opção de ocultar o agente de VPN instalado no cliente remoto, tornando o mesmo invisível para o usuário;
- g.12)** Deve exibir mensagens de notificação customizada toda vez que um usuário remoto se conectar a VPN. Deve permitir que o usuário desabilite a exibição da mensagem nas conexões seguintes;
- g.13)** Deve avisar ao usuário remoto de VPN quanto a proximidade da expiração de senha LDAP. Deve permitir também a customização da mensagem com informações relevantes para o usuário;
- g.14)** Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
- g.15)** A VPN SSL deve suportar proxy arp e uso de interfaces PPPoE;
- g.16)** Suportar autenticação via AD/LDAP, OTP (One Time Password), certificado e base de usuários local;
- g.17)** Deve permitir a distribuição de certificado para o usuário de remoto através do portal de VPN de forma automatizada;
- g.18)** Deve possuir lista de bloqueio para dispositivos em casos quando, por exemplo, o usuário reportar que o dispositivo foi perdido ou roubado;
- g.19)** Permite estabelecer um túnel VPN client-to-site do cliente a plataforma de segurança, fornecendo uma solução de single-sign-on aos usuários, integrando-se com as ferramentas de Windows-logon;
- g.20)** Suporta leitura e verificação de CRL (certificate revocation list);
- g.21)** Permite a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;
- g.22)** agente de VPN a ser instalado nos equipamentos desktop e laptops, dever ser capaz de ser distribuído de maneira automática via Microsoft SMS, Active Directory e ser descarregado diretamente desde o seu próprio portal, o qual residirá no centralizador de VPN;
- g.23)** agente deverá comunicar-se com o portal para determinar as políticas de segurança do usuário,
- g.24)** Deve permitir que a conexão com a VPN SSL seja estabelecida das

[Handwritten signature]

	<p>seguintes formas:</p> <ul style="list-style-type: none"> ✓ Antes do usuário autenticar na estação; ✓ Após autenticação do usuário na estação; ✓ Sob demanda do usuário; <p>g.25) Deverá manter uma conexão segura com o portal durante a sessão.</p> <p>g.26) O agente de VPN SSL client-to-site deve ser compatível com pelo menos: Windows XP, Vista Windows 7, Windows 8, Mac OSx e Chrome OS;</p>
1.14	<p>COMPATIBILIDADE</p> <p>a) A padronização da marca garante que os equipamentos adquiridos pelo MP/PI sejam 100% compatíveis entre si, permitindo a proteção de investimento já realizado por este órgão. Desta forma, faz-se necessário a aquisição de firewall de mesma marca e modelo para que possam operar em Alta Disponibilidade e também ser gerenciado pela solução já existente no MP/PI.</p> <p>b) Equipamento ofertado deverá ser compatível com software de gerenciamento PANORAMA adquirido pelo MP/PI;</p> <p>c) Marca e modelo para referência: Palo Alto PA-3020;</p>
1.15	<p>SERVIÇO DE INSTALAÇÃO/CONFIGURAÇÃO</p> <p>a) Prestar serviços de instalação e configuração, que compreendem, entre outros, os seguintes procedimentos:</p> <p>b) Instalação e configuração de firewalls em Alta Disponibilidade (ativo/passivo) no seguinte endereço Campus Marco Zero – Macapá Rod. uscelino ubirischeck, M 02 ardim Marco Zero Macapá – AP – CEP 68903-419;</p> <p>c) Análise da topologia e arquitetura da rede, considerando os roteadores e switches já existentes instalados;</p> <p>d) Análise do acesso Internet, sites remotos, serviços de rede oferecidos aos funcionários e aos usuários externos;</p> <p>e) Regras de Firewall existentes e aplicáveis solução ofertada dada a colocação desta na Rede da U IFAP;</p> <p>f) Análise do posicionamento de qualquer outro equipamento ou sistema relevante na segurança de qualquer perímetro protegido pela solução;</p> <p>g) Instalação física de todos os equipamentos adquiridos no local determinado pela equipe de TI;</p> <p>h) Configuração do sistema de Firewall, VPN, IPS, Filtro URL, Antivírus e Anti malware de acordo com as exigências levantadas;</p> <p>i) Adicionar equipamentos no sistema de gerenciamento Palo Alto Panorama já existente no MP/PI;</p> <p>j) Repasse no formato hands-on de 04 (quarto) horas para o NTI após validação da migração;</p> <p>k) Deve haver geração de relatório com as configurações efetuadas e as decisões tomadas em formato legível e tecnicamente fundamentado;</p> <p>l) Deverá ser considerado 08 (oito) horas adicionais pós implementação que poderá ser utilizado para fins de suporte, manutenção, atualização e dúvidas referente aos equipamentos deste grupo. Será aceito atendimento remoto</p>

[Handwritten signature]

	para esta finalidade.
--	-----------------------

CLÁUSULA TERCEIRA - DA DOTAÇÃO ORÇAMENTÁRIA

3.1 A despesa correrá à conta da seguinte dotação orçamentária:

- Unidade Orçamentária: 25101
- Função: 03
- Programa: 82
- Projeto/Atividade: 2400
- Fonte de Recursos: 00
- Natureza da Despesa: 4.4.90.52

CLÁUSULA QUARTA - DO VALOR DO CONTRATO

4.1 O valor total do Contrato é de **R\$370.000,00** (trezentos e setenta mil reais), devendo a importância de **R\$370.000,00** (trezentos e setenta mil reais) ser atendida à conta de dotações orçamentárias consignadas no orçamento corrente - Lei Orçamentária Anual de 2016.

CLÁUSULA QUINTA - DA GARANTIA

5.1 Durante o prazo de 36 meses, deve ser possível realizar a atualização de sistema operacional dos equipamentos, incluindo atualizações de novas assinaturas;

5.2 A garantia deve incluir envio de peças ou equipamentos de reposição nos locais especificados neste termo de referência, obedecendo a modalidade NBD (Next Business Day);

5.3 Os chamados poderão ser abertos diretamente com o fabricante ou autorizada pelo fabricante através de ligação telefônica 0800 no idioma Português. Também deverá ser possível abertura de chamados via website e/ou e-mail durante a vigência da garantia (36 meses). O suporte deverá ser na modalidade de 24x7 (24 horas por dia, 7 dias por semana), com atendimento através de ligação telefônica para atendimentos emergenciais;



CLÁUSULA SEXTA – DO LOCAL E DOS PRAZOS DE ENTREGA

6.1 O prazo de entrega de produtos deverá ocorrer em até no máximo 30 (noventa) dias corridos a partir da data de assinatura do contrato; Será admitida a prorrogação do prazo uma única vez por igual período, mediante a apresentação de justificativa devidamente aceita pela autoridade competente;

6.2 A entrega deve ser agendada com antecedência mínima de 24 (vinte e quatro) horas, sob o risco de não ser autorizada;

6.3 Para itens de software, poderá ser fornecido sem mídia de instalação, desde que seja indicado local para download do arquivo de instalação;

6.4 O local de entrega será na Coordenadoria de Tecnologia da Informação, localizado na Rua Álvaro Mendes, nº 2294, CEP: 64.000-060, Teresina-PI.

CLÁUSULA SÉTIMA – DA VIGÊNCIA E DA EFICÁCIA

7.1 O contrato terá a duração de 12 (doze) meses, contados da data de sua assinatura, podendo prorrogado por iguais e sucessivos períodos até o limite de 48 (quarenta e oito) meses, nos termos do artigo 57, IV, da Lei 8.666/93, tendo eficácia após a publicação do extrato do ato no Diário de Justiça do Estado do Piauí, nos termos do art. 61, parágrafo único da Lei 8.666/1993.

CLÁUSULA OITAVA – DO RECEBIMENTO DOS SERVIÇOS

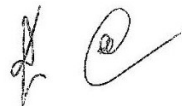
8.1. Os serviços serão considerados prestados e aceitos após o atesto no documento fiscal pelo servidor competente, comprovando que não houve quaisquer transtornos na execução do serviço.

8.2. O servidor terá o prazo de 5 (cinco) dias úteis, após o recebimento do documento fiscal, para se manifestar quanto a execução do serviço.

8.3. A CONTRATADA deverá apresentar ao ÓRGÃO CONTRATANTE a documentação que comprove a prestação do serviço, juntamente com a Nota Fiscal para o correspondente pagamento dos serviços executados.

CLÁUSULA NONA – DO REAJUSTE

9.1 O preço consignado neste contrato, será corrigido anualmente, observado o interregno mínimo de um ano, contado a partir da data limite para a apresentação da proposta, pela variação do **Índice Nacional de Preços ao Consumidor – INPC/IBGE** ou outro índice que venha a substituí-lo.



9.1.1 Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

CLÁUSULA DÉCIMA - DAS OBRIGAÇÕES DA CONTRATADA

10.1. Efetuar a entrega dos itens em perfeitas condições, na Coordenadoria de Tecnologia da Informação, no prazo máximo de 30 (trinta) dias corridos, contados da data da assinatura do Contrato. Será admitida a prorrogação do prazo uma única vez por igual período, mediante a apresentação de justificativa devidamente aceita pela autoridade competente;

10.2. Substituir os itens que apresentarem vícios redibitórios, em definitivo, no prazo máximo de 20 (vinte) dias corridos, contados da constatação da necessidade, sem que dessa troca decorra qualquer ônus para a Contratante;

10.3. Responsabilizar-se por quaisquer despesas decorrentes da execução de entrega de qualquer item (inclusive pelo transporte quando da necessidade de remoção), bem como, substituição de qualquer item defeituoso, sem ônus para a Contratante;

10.4. Responsabilizar-se pelos danos causados à Contratante ou a terceiros, decorrentes de sua culpa e/ou dolo quando da entrega dos itens;

10.5. Manter, durante o período da garantia, todas as condições que ensejaram sua habilitação no presente pregão.

10.6 Somente serão aceitos equipamentos novos e sem uso. Não serão aceitos equipamentos re-manufaturados, NFR (Not For Resale) ou de demonstração. Os equipamentos deverão ser entregues nas caixas lacradas pelo fabricante, não sendo aceitos equipamentos com caixas violadas;

10.7 O aceite do bem somente será dado após comprovação da entrega e o efetivo cumprimento de todas as exigências da presente especificação técnica;

10.8 Será consultado diretamente no site do fabricante do equipamento manuais e toda documentação pública disponível para comprovação do pleno atendimento aos requisitos deste edital. Em caso de dúvida ou divergência na comprovação da especificação técnica, este órgão poderá solicitar amostra do equipamento ofertado, sem ônus ao processo, para comprovação técnica de funcionalidades. Esta amostra deverá ocorrer em até 15 (quinze) dias úteis após a solicitação deste órgão. Para a amostra, a empresa deverá apresentar o mesmo modelo do equipamento ofertado no certame, com técnico certificado na solução para configuração e comprovação dos itens pendentes, nas dependências deste órgão



[conforme itens 1.1.1 e 1.1.2, TC-006.806/2006-4, Acórdão nº 838/2006-TCU-2ª Câmara];

CLÁUSULA DÉCIMA PRIMEIRA - OBRIGAÇÕES DO MINISTÉRIO PÚBLICO DO ESTADO DO PIAUÍ

- 11.1. Exigir o cumprimento de todos os compromissos assumidos pelo FORNECEDOR de acordo com este contrato e os termos de sua proposta;
- 11.2. Efetuar o pagamento dentro do prazo previsto na cláusula décima segunda, a contar do recebimento do recebimento definitivo dos objetos;
- 11.3. Notificar o FORNECEDOR, por escrito, sobre imperfeições, falhas ou irregularidades constatadas nos itens, para que sejam adotadas as medidas corretivas necessárias.
- 11.4. A Contratante poderá deduzir do montante a pagar os valores correspondentes a multas ou indenizações devidas pela licitante vencedora, nos termos do Edital.

CLÁUSULA DÉCIMA SEGUNDA- DO PAGAMENTO

- 12.1. O pagamento a favor do licitante vencedor será efetuado até o 10º (décimo) dia útil, após o recebimento definitivo e aceitação dos serviços, mediante a apresentação da respectiva **nota fiscal/fatura** devidamente atestada pelo setor competente, observada a ordem cronológica estabelecida no artigo 5º da Lei nº 8.666/93. Para os fins de pagamento ainda será solicitada a apresentação das certidões negativas de débitos relativas ao FGTS, à previdência, ao trabalho, situação fiscal tributária federal, certidão negativa de tributos estaduais e municipais, mantendo-se as mesmas condições de habilitação do certame, sendo que as mesmas deverão sempre apresentar data de validade posterior à data de emissão das respectivas Notas Fiscais.
- 12.2. Na ocorrência de rejeição da(s) Nota(s) Fiscal(is), motivada por erro ou incorreções, o prazo para pagamento passará a ser contado a partir da data da sua reapresentação.
- 12.3. Se houver atraso após o prazo previsto, as faturas serão pagas acrescidas de juros de mora de 6% (seis por cento) ao ano, aplicados *pro rata die* da data do vencimento até o efetivo pagamento, desde que solicitado pela Empresa.
 - 12.3.1 O valor dos encargos será calculado pela fórmula: $EM = I \times N \times VP$, onde: EM = Encargos moratórios devidos; N = Números de dias entre a data



prevista para o pagamento e a do efetivo pagamento; I = Índice de compensação financeira = 0,00016438; e VP = Valor da prestação em atraso.

12.4. Nenhum pagamento será efetuado à licitante vencedora enquanto pendente de liquidação qualquer obrigação financeira, sem que isso gere direito à alteração de preços ou a compensação financeira.

12.5. A Procuradoria Geral de Justiça reserva-se o direito de recusar o pagamento se, no ato da atestação, o objeto não estiver de acordo com as especificações apresentadas e aceitas.

12.6. O pagamento será feito por meio de ordem bancária em conta a ser indicada pela contratada cuja ordem bancária dará quitação ao pagamento, e nos termos da lei, será debitado do valor devido ao MP/PI, referente aos serviços prestados, os valores relativos aos tributos e contribuições sociais.

12.7. O CNPJ contido na nota fiscal/fatura emitida pela Contratada deverá ser o mesmo que estiver registrado no contrato celebrado ou instrumento equivalente, independentemente da favorecida ser matriz, filial, sucursal ou agência.

12.8. A Administração poderá descontar do valor do pagamento que o fornecedor tiver a receber, importâncias que lhe sejam devidas, por força da aplicação das multas previstas na Cláusula Décima Terceira.

CLÁUSULA DECIMA TERCEIRA - DAS SANÇÕES ADMINISTRATIVAS:

13.1 Com fundamento no artigo 7º da Lei nº 10.520/2002, ficará impedida de licitar e contratar com o Estado do Piauí e será descredenciada do Cadastro Único de Fornecedores de Materiais, Bens e Serviços para a Administração Direta e Indireta do Estado do Piauí (CADUF), pelo **prazo de até 5 (cinco) anos**, garantida a ampla defesa, sem prejuízo da rescisão unilateral do contrato e da aplicação de multa de **até 30% (trinta por cento)** sobre o valor total da contratação, a CONTRATADA que:

13.1.1 Cometer fraude fiscal;

13.1.2 Apresentar documento falso;

13.1.3 Fizer declaração falsa;

13.1.4 Comportar-se de modo inidôneo;

13.1.5 Não retirar a nota de empenho ou não assinar o contrato, nos prazos estabelecidos;

13.1.6 Deixar de entregar a documentação exigida no certame;



13.1.7 Não manter a proposta.

13.2. Para os fins do item 13.1.4, reputar-se-ão inidôneos atos tais como os descritos nos artigos 92, parágrafo único, 96 e 97, parágrafo único, da Lei nº 8.666/1993.

13.3. Com fundamento nos artigos 86 e 87, incisos I a IV, da Lei nº 8.666, de 1993; e no art. 7º da Lei nº 10.520, de 17/07/2002, nos casos de retardamento, de falha na execução do contrato ou de inexecução total do objeto, garantida a ampla defesa, a CONTRATADA poderá ser apenada, isoladamente, ou juntamente com as multas definidas nos itens "13.4", "13.6", "13.7" e "13.9" abaixo, com as seguintes penalidades:

13.3.1. Advertência;

13.3.2. Suspensão temporária de participação em licitação e impedimento de contratar com a Administração do Ministério Público do Estado do Piauí (MP-PI), por prazo não superior a 2 (dois) anos;

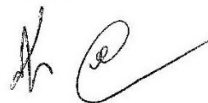
13.3.3. Declaração de inidoneidade para licitar ou contratar com a Administração Pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a CONTRATADA ressarcir a Administração pelos prejuízos resultantes e após decorrido o prazo da sanção aplicada com base no inciso anterior; ou

13.3.4. Impedimento de licitar e contratar com o Estado do Piauí e descredenciamento no CADUF, ou nos sistemas de cadastramento de fornecedores a que se refere o inciso XIV do art. 4º da Lei nº 10.520/2002, pelo prazo de até 5 (cinco) anos.

13.4. No caso de inexecução total do serviço, garantida a ampla defesa e o contraditório, a CONTRATADA estará sujeita à aplicação de multa de até 30% (trinta por cento) do valor total do contrato.

13.5. Configurar-se-á a inexecução total do serviço quando, decorridos 15 (quinze) dias do término do prazo estabelecido para execução do contrato, nenhuma unidade do objeto for entregue pela CONTRATADA. **Neste caso, a Administração poderá cobrar valor excedente a este percentual se os prejuízos sofridos superarem o montante da multa aplicada, com supedâneo no artigo 416 do CC/02.**

13.6. Em caso de retardamento na execução do serviço, será aplicada multa de



1% (um por cento) do valor unitário do bem em atraso, por dia, por unidade, até o limite de 20% do valor unitário do serviço.

13.7. No caso de inexecução parcial do serviço ou de descumprimento de obrigação contratual, garantida a ampla defesa e o contraditório, a CONTRATADA estará sujeita à aplicação de multa de até 20% (vinte por cento) do valor total do contrato.

13.8. Configurar-se-á a inexecução parcial do serviço quando, decorridos 15 (quinze) dias do término do prazo estabelecido para execução do contrato, houver prestação do serviço pela CONTRATADA, mas não em sua totalidade.

13.9. As multas decorrentes de retardamento na execução do serviço poderão ser aplicadas juntamente às multas por inexecução parcial ou total do serviço, às multas por descumprimento de obrigação contratual.

13.10. O valor da multa poderá ser descontado das faturas devidas à CONTRATADA.

13.10.1. Se os valores das faturas forem insuficientes, fica a CONTRATADA obrigada a recolher a importância devida no prazo de 15 (quinze) dias, contados da comunicação oficial.

13.10.2. Esgotados os meios administrativos para cobrança do valor devido pela CONTRATADA à CONTRATANTE, este será encaminhado para inscrição em dívida ativa.

13.11. O contrato, sem prejuízo das multas e demais cominações legais previstas no contrato, poderá ser rescindido unilateralmente, por ato formal da Administração, nos casos enumerados no art. 78, incisos I a XII e XVII, da Lei nº 8.666/93.

CLÁUSULA DÉCIMA QUARTA - DA RESCISÃO

14.1 A inexecução total ou parcial do contrato poderá ensejar a sua rescisão, com as consequências contratuais e as previstas em lei.

14.2 Constituem motivos de rescisão do contrato, independentemente de notificação ou interpelação judicial:

14.2.1 O descumprimento ou cumprimento irregular, pela contratada, de quaisquer das obrigações/responsabilidades relevantes que acarretem prejuízos ao interesse público, bem como das condições previstas no edital e no contrato.

14.2.2 A subcontratação total ou parcial do seu objeto, a associação do



contratado com outrem, a cessão ou transferência, total ou parcial, bem como a fusão, cisão ou incorporação, não admitidas no edital ou no contrato;

14.2.3 O cometimento reiterado de faltas ou defeitos na execução do pactuado;

14.2.4 A decretação de falência ou insolvência civil da contratada;

14.2.5 A dissolução da sociedade;

14.2.6 A alteração societária, do objeto social ou modificação da finalidade ou da estrutura da empresa que, a juízo da PROCURADORIA, prejudique a aquisição contratada;

14.2.7 O atraso injustificado na execução dos serviços descritos no contrato após a devida notificação da contratada;

14.2.8 A paralização, total ou parcial, do objeto descrito no Contrato, sem justa causa e prévia comunicação à PROCURADORIA;

14.2.9 O desatendimento das determinações regulares da autoridade designada para acompanhar e fiscalizar a sua execução, assim como as de seus superiores;

14.2.10 A lentidão no seu cumprimento, levando a PROCURADORIA a comprovar a impossibilidade da conclusão da prestação dos serviços;

14.2.11 Razões de interesse público, de alta relevância e amplo conhecimento, justificadas e determinadas pela máxima autoridade da esfera administrativa a que está subordinada a PROCURADORIA e exaradas no processo administrativo a que se refere o contrato;

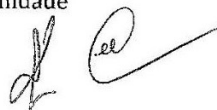
14.2.12 A ocorrência de caso fortuito ou de força maior, regularmente comprovada, impeditiva da prestação dos serviços;

14.2.13 O conhecimento posterior de qualquer fato ou de circunstância superveniente que desabone ou que afete a idoneidade ou a capacidade técnica ou financeira da empresa participante implicará necessariamente na rescisão contratual, se o contrato já tiver sido assinado.

14.3 Os casos de rescisão a seguir discriminados dependem de interposição judicial para a sua execução, assegurando-se o contraditório e a ampla defesa:

14.3.1 A supressão, por parte da Administração, de obras, serviços ou compras, acarretando modificação do valor inicial do contrato além do limite permitido no § 1º do art. 65 desta Lei;

14.3.2 A suspensão de sua execução, por ordem escrita da Administração, por prazo superior a 120 (cento e vinte) dias, salvo em caso de calamidade



pública, grave perturbação da ordem interna ou guerra, ou ainda por repetidas suspensões que totalizem o mesmo prazo, independentemente do pagamento obrigatório de indenizações pelas sucessivas e contratualmente imprevistas desmobilizações e mobilizações e outras previstas, assegurado ao contratado, nesses casos, o direito de optar pela suspensão do cumprimento das obrigações assumidas até que seja normalizada a situação;

14.3.3 O atraso superior a 90 (noventa) dias dos pagamentos devidos pela Administração decorrente da prestação dos serviços, ou parcelas destes, já recebidos ou executados, salvo em caso de calamidade pública, grave perturbação da ordem interna ou guerra, assegurado ao contratado o direito de optar pela suspensão do cumprimento de suas obrigações até que seja normalizada a situação;

14.3.4 A não liberação, por parte da Administração, de área, local ou objeto para a prestação dos serviços, nos prazos contratuais, bem como das fontes de materiais naturais especificadas no projeto;

14.4 Verificada a rescisão contratual, cessarão automaticamente todas as atividades da contratada relativas à prestação dos serviços descritos no Contrato.

14.5 Os casos de rescisão contratual serão formalmente motivados nos autos do processo, assegurados o contraditório e a ampla defesa;

14.6 No caso de rescisão provocada por inadimplemento da CONTRATADA, a CONTRATANTE poderá reter, cautelarmente, os créditos decorrentes do contrato até o valor dos prejuízos causados, já calculados ou estimados.

CLÁUSULA DÉCIMA QUINTA – DA DISSOLUÇÃO

15.1 O Contrato poderá ser dissolvido de comum acordo, bastando, para tanto, manifestação escrita de uma das partes, com antecedência mínima de 60 (sessenta) dias, sem interrupção do curso normal da execução do Contrato.

CLÁUSULA DÉCIMA SEXTA – DOS DÉBITOS PARA COM A FAZENDA PÚBLICA

16.1 Os débitos da CONTRATADA para com o MP/PI, decorrentes ou não do ajuste, serão inscritos em Dívida Ativa e cobrados mediante execução na forma da legislação pertinente, podendo, quando for o caso, ensejar a rescisão unilateral do Contrato.



CLÁUSULA DÉCIMA SÉTIMA- DO FISCAL DO CONTRATO

17.1 A Coordenadoria de Tecnologia da Informação indicará servidor responsável pela fiscalização do contrato, nos moldes do artigo 67 da Lei nº 8.666/93 e do Ato PGJ nº 462/2013. Oportunamente, a Procuradora-Geral de Justiça ficará encarregada da designação do fiscal para o exercício das atribuições que lhe são inerentes durante o prazo de vigência do contrato.


CLÁUSULA DÉCIMA OITAVA - DA PUBLICAÇÃO E DO REGISTRO

18.1 A eficácia do Contrato fica condicionada à publicação resumida do instrumento pela Administração, no Diário da Justiça do Estado do Piauí, até o quinto dia útil do mês seguinte ao de sua assinatura, para ocorrer no prazo de vinte dias daquela data.

CLÁUSULA DÉCIMA NONA - DO FORO



19.1 Fica eleito o foro de Teresina-PI, para dirimir quaisquer dúvidas relativas ao cumprimento do presente Contrato.

Teresina, 22 de dezembro de 2016.


Zélia Saraiva Lima
Procuradora-Geral de Justiça em exercício


Kent Johann Modes
Empresa Approach Tecnologia Ltda

Testemunhas

1  CPF 746.005.913-72
2  CPF 251.034.338-69



Diário da Justiça do Estado do Piauí

ANO XXXIX - Nº 8126 Disponibilização: Quinta-feira, 12 de Janeiro de 2017 Publicação: Sexta-feira, 13 de Janeiro de 2017

- d) **Processo Administrativo:** nº 26.609/2016;
e) **Processo Licitatório:** Adesão nº 23/2016/MP/PI, ao Sistema de Registro de Preço oriundo da licitação realizada na modalidade Pregão nº 05/2016/MP/RO, executado na forma eletrônica, que gerou a Ata de Registro de Preço nº 05/2016.
f) **Vigência:** O contrato terá vigência de 12 (doze) meses a partir da data de publicação, podendo ser prorrogado, por juízo de conveniência e oportunidade pela Administração Pública, até o limite de 60 (sessenta) meses.
g) **Valor:** R\$ 33.458,40 (trinta e três mil, quatrocentos e oitenta reais e quarenta centavos), sendo o valor mensal de R\$ 2.788,20 (dois mil, setecentos e oitenta e oito reais e vinte centavos).
h) **Cobertura orçamentária:** Unidade Orçamentária: 25101; Fonte de Recursos: 00; Natureza da Despesa: 3.3.90.39; Empenho: 2016NE01872;
i) **Signatários:** pela **contrata:** Eduardo Leite Cruz Lacet, inscrito no CPF sob o nº 010.362.674-31, e **contratante,** Dra. Zélia Saraiva Lima, Procuradora-Geral de Justiça em exercício.

ANEXO I

Item	Discriminação	Unid	Qtd	Valor unitário	Valor Mensal	Valor Total
01	Serviço de rastreamento e monitoramento 24 horas, em tempo real, de veículos da frota do Ministério Público do Estado do Piauí, em mapas digitais e imagens de satélite, por meio de sistemas GPS/GSM/GPRS, incluindo o fornecimento e serviços de instalação, treinamento de pessoas para operar o sistema, licença e manutenção de sistemas (software) e equipamentos de rastreamento automotivo (módulos) em regime de comodato, em todo o Estado do Piauí (capital e interior), conforme especificações constantes do Termo de Referência n. 001/SESTRAN/MP/2016.	Unid	60	46,47	2.788,20	33.458,40
Valor Total do Item					2.788,20	33.458,40

Teresina, 12 de janeiro de 2017.

10.2. EXTRATO DO CONTRATO Nº 04/2016

PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE LICITAÇÕES E CONTRATOS
EXTRATO DO CONTRATO Nº 04/2016

- a) **Espécie:** Contrato nº 04/2016, firmado em 22 de dezembro de 2016, entre o Fundo Estadual de Proteção e Defesa do Consumidor - FPDC, CNPJ nº 24.291.901/0001-48 e a empresa TCA TRANSFORMAÇÕES VEICULARES LTDA., CNPJ nº 08.389.661/0001-62;
b) **Objeto:** Aquisição de ônibus tipo rodoviário adaptado, composto por chassi e transformações para funcionar como unidade móvel de atendimento para Promotoria Itinerante do MP/PI.
c) **Fundamento Legal:** Lei 8.666/93;
d) **Processo Administrativo:** nº 28.013/2016;
e) **Processo Licitatório:** Pregão Eletrônico nº 43/2016, Ata de Registro de Preços nº 44/2016.
f) **Vigência:** O contrato terá sua vigência de 12 (doze) meses, a contar da data de sua assinatura, com eficácia a contar da data de sua correspondente publicação no Diário da Justiça do Estado do Piauí.
g) **Valor:** R\$ 850.000,00 (oitocentos e cinquenta mil reais).
h) **Cobertura orçamentária:** Unidade Orçamentária: 25104; Fonte de Recursos: 18; Natureza da Despesa: 4.4.90.52; Empenho: 2016NE00007;
i) **Signatários:** pela **contrata:** Claudionor Antônio Tasca, inscrito no CPF sob o nº 476.481.120-00, e **contratante,** Dr. Nivaldo Ribeiro, Presidente do Conselho Gestor do FPDC.

ANEXO I

ITEM	OBJETO	QTD	VALOR UNITÁRIO
I	Ônibus adaptados para Promotoria Itinerante. Chassi Marca: Volkswagen; Modelo: Volkswagen 18.330 OT; Carroceria: Mascarello / Modelo Roma M4 VERSÃO STD, Adaptados para Promotoria Itinerante.	1	R\$850.000,00

Teresina, 12 de janeiro de 2017.

10.3. EXTRATO DO CONTRATO Nº 77/2016

PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE LICITAÇÕES E CONTRATOS
EXTRATO DO CONTRATO Nº 77/2016

- a) **Espécie:** Contrato nº 77/2016, firmado em 22 de dezembro de 2016, entre a Procuradoria Geral de Justiça do Estado do Piauí - CNPJ 05.805.924/0001-89 e a empresa EMPRESA APPROACH TECNOLOGIA LTDA, CNPJ nº 24.376.542/0001-21;
b) **Objeto:** Contrato de Adesão nº 22/2016, à Ata de Registro de Preços nº 128/2016 da Universidade Federal do Amapá - UNIFAP, para aquisição de Firewall para prover proteção aos servidores, estação de trabalho e demais dispositivos conectados à rede com conexões originadas ou destinadas à internet do MP/PI.
c) **Fundamento Legal:** Lei 8.666/93;
d) **Processo Administrativo:** nº 27.090/2016;
e) **Processo Licitatório:** Adesão nº 22/2016, à Ata de Registro de Preços nº 128/2016 da Universidade Federal do Amapá - UNIFAP;
f) **Vigência:** O contrato terá a duração de 12 (doze) meses, contados da data de sua assinatura, podendo ser prorrogado por iguais e sucessivos períodos até o limite de 48 (quarenta e oito) meses, nos termos do artigo 57, IV, da Lei 8.666/93, tendo eficácia após a publicação do extrato do ato no Diário da Justiça do Estado do Piauí, nos termos do art. 61, parágrafo único da Lei 8.666/1993.
g) **Valor:** R\$370.000,00 (trezentos e setenta mil reais).
h) **Cobertura orçamentária:** Unidade Orçamentária: 25101; Fonte de Recursos: 00; Natureza da Despesa: 4.4.90.52; Empenho: 2016NE01871;
i) **Signatários:** pela **contrata:** Rogério Francisco dos Santos, inscrito no CPF sob o nº [REDACTED] e **contratante,** Dra. Zélia Saraiva Lima, Procuradora-Geral de Justiça em exercício.

ANEXO I

ITEM	QTD	DESCRIÇÃO	VALOR UNITÁRIO	VALOR TOTAL
------	-----	-----------	----------------	-------------



Diário da Justiça do Estado do Piauí

ANO XXXIX - Nº 8126 Disponibilização: Quinta-feira, 12 de Janeiro de 2017 Publicação: Sexta-feira, 13 de Janeiro de 2017

1	2	FIREWALL TIPO 1 com instalação/configuração	R\$185.000,00	R\$370.000,00
---	---	---	---------------	---------------

Teresina, 12 de janeiro de 2017.

10.4. EXTRATO DO CONTRATO Nº 05/2016

PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE LICITAÇÕES E CONTRATOS

EXTRATO DO CONTRATO Nº 05/2016

- a) **Espécie:** Contrato nº 05/2016, firmado em 22 de dezembro de 2016, entre o Fundo Estadual de Proteção e Defesa do Consumidor - FPDC, CNPJ nº 24.291.901/0001-48 e a empresa **CIRO NOGUEIRA COMÉRCIO DE MOTOCICLETAS LTDA.**, CNPJ nº 02.297.980/0010-52;
b) **Objeto:** Aquisição de motocicletas de 125 cilindradas, conforme as quantidades e especificações contidas no Anexo I e no edital do Pregão Eletrônico nº 35/2016.
c) **Fundamento Legal:** Lei 8.666/93;
d) **Processo Administrativo:** nº 15.505/2016;
e) **Processo Licitatório:** Pregão Eletrônico nº 35/2016, Ata de Registro de Preços nº 40/2016.
f) **Vigência:** O contrato terá sua vigência de 12 (doze) meses, a contar da data de sua assinatura, com eficácia a contar da data de sua correspondente publicação no Diário da Justiça do Estado do Piauí.
g) **Valor:** R\$47.336,10 (quarenta e sete mil e trezentos e trinta e seis reais e dez centavos).
h) **Cobertura orçamentária:** Unidade Orçamentária: 25104; Fonte de Recursos: 18; Natureza da Despesa: 4.4.90.52; Empenho: 2016NE00004;
i) **Signatários:** pela **contrata:** Luciano de Castro Koury, inscrito no CPF sob o nº 504.289.423-34, e **contratante,** Dr. Nivaldo Ribeiro, Presidente do Conselho Gestor do FPDC.

ANEXO I

Item	Descrição do objeto	Qtd	Valor Unitário
1	<p>-Motocicleta, com motor 4 tempos.</p> <p>- 125 cilindradas aproximadamente, 0 Km;</p> <p>-Sistema de alimentação: Injeção eletrônica e partida elétrica ou por pedal;</p> <p>-Data de fabricação/modelo igual ou posterior à data de realização do certame;</p> <p>- Cor: preto metálico;</p> <p>- Gasolina ou gasolina e álcool.</p> <p>- Assento em material impermeável, na cor preta, reforçado para suportar o uso contínuo de passageiro com peso de pelo menos 90 kg;</p> <p>- Freio a disco na roda dianteira ou a tambor</p> <p>-Capacidade do tanque de pelo menos 10 (dez) litros de combustível;</p> <p>-Pneus com aro 18.</p> <p>-Pneu dianteiro 80/80-18 M/C ou 80/100-18 M/C ou 2.75-18 M/C</p> <p>-Pneu traseiro 90/90-18 M/C aproximadamente;</p> <p>-Farol fixo no guidão, permitindo que a luminosidade emitida pelo conjunto do farol se movimente de acordo com as manobras exercidas pelo piloto.</p> <p>- Transmissão 5 (cinco) velocidades;</p> <p>-Dispositivo contra "linha de pipa", equipamento de proteção para integridade física do condutor, constituída de vareta telescópica, com cerca de 01 (um) metro de comprimento, confeccionado em material resistente e flexível, com sistema que permita o corte da linha nas extremidades. Deverá ser instalado na mela extremidade do guidão ou carenagem da motocicleta, de modo a não causar ferimentos ao condutor em caso de acidentes com a motocicleta;</p> <p>-Demais equipamentos e acessórios obrigatórios previstos pelas leis e normas brasileiras de trânsito.</p> <p>Garantia de no mínimo 1(um) ano;</p> <p>PRAZO DE ENTREGA: 90 DIAS CORRIDOS</p> <p>Marca/Modelo: Honda tipo Fan 125i.</p>	6	R \$ 7.889, 35

Teresina, 12 de janeiro de 2017.

10.5. EXTRATO DO CONTRATO Nº 07/2016

PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE LICITAÇÕES E CONTRATOS

EXTRATO DO CONTRATO Nº 07/2016

- a) **Espécie:** Contrato nº 07/2016, firmado em 22 de dezembro de 2016, entre o Fundo Estadual de Proteção e Defesa do Consumidor - FPDC, CNPJ nº 24.291.901/0001-48 e a empresa **HPE AUTOMOTORES DO BRASIL LTDA.**, CNPJ nº 54.305.743/0011-70;
b) **Objeto:** Aquisição de veículos novos, zero quilômetro, tipo Pick-Up, conforme as quantidades e especificações contidas no Anexo I e no edital do Pregão Eletrônico nº 35/2016.
c) **Fundamento Legal:** Lei 8.666/93;
d) **Processo Administrativo:** nº 15.505/2016;
e) **Processo Licitatório:** Pregão Eletrônico nº 35/2016, Ata de Registro de Preços nº 43/2016.
f) **Vigência:** O contrato terá sua vigência de 12 (doze) meses, a contar da data de sua assinatura, com eficácia a contar da data de sua correspondente publicação no Diário da Justiça do Estado do Piauí.
g) **Valor:** R\$ 111.500,00 (Cento e onze mil e quinhentos reais).
h) **Cobertura orçamentária:** Unidade Orçamentária: 25104; Fonte de Recursos: 18; Natureza da Despesa: 4.4.90.52; Empenho: 2016NE00005;
i) **Signatários:** pela **contrata:** Eduardo Cordeiro de Almeida e Silva, inscrito no CPF sob o nº 157.699.348-59, e **contratante,** Dr. Nivaldo Ribeiro, Presidente do Conselho Gestor do FPDC.

ANEXO I

Item	Descrição do objeto	Qtd	Valor Unitário
1	<p>-Veículo tipo Pick Up - Dupla Cabine - 4x2 ou 4x4, zero quilômetro, com capacidade para 05(cinco) passageiros. 4 portas;</p> <p>-Cor: Preta</p>	01	R \$ 111.500, 00