CONTRATO Nº. 091/2021-MP/PA

CONTRATO QUE ENTRE SI FAZEM O MINISTÉRIO PÚBLICO DO ESTADO DO PARÁ E A EMPRESA SIGMAFONE TELECOMUNICAÇÕES LTDA.

MINISTÉRIO PÚBLICO DO ESTADO DO PARÁ, inscrito no CNPJ/MF sob o nº 05.054.960/0001-58, estabelecido nesta Cidade à Rua João Diogo, 100, bairro Cidade Velha, CEP: 66015-165, doravante denominado **CONTRATANTE**, neste ato representado pelo Procurador-Geral de Justiça, Exmo. Sr. Dr. **CESAR BECHARA NADER MATTAR JUNIOR**, brasileiro, residente e domiciliado em Belém e, de outro lado, a Empresa **SIGMAFONE TELECOMUNICAÇÕES LTDA,** Nome Fantasia: **SIGMA TELECOM**, pessoa jurídica de direito privado, portadora do CNPJ/MF nº78.766.151/0001-42**,** Inscrição Estadual nº 1016213248, estabelecida à Rua Anita Ribas, nº 365, Bairro Bacacheri, Município de Curitiba – PR, CEP 82.520-610, e-mail: borges@sigmatelecom.com.br, comercial@sigmatelecom.com.br, telefone (41) 3360-6677, neste ato representada pelo Sr. **REYNALDO COSTA E ROSA**, brasileiro, casado, administrador de empresas, inscrito no CPF sob o nº 901.580.755-87, residente e domiciliado Município de Curitiba – PR, doravante denominada **CONTRATADA**, têm por justo e contratado o que melhor se declara nas cláusulas e condições seguintes:

CLÁUSULA PRIMEIRA - DO FUNDAMENTO JURÍDICO

1.1. O presente Contrato decorre de licitação na modalidade **Pregão Eletrônico Nº 047/2020-MP/PA**, por execução indireta, empreitada por preço **global do lote/grupo**, no tipo menor preço, vinculada ao **PROCESSO Nº. 162/2019-SGJ-TA (PROTOCOLO N° 45212/2019) e Ata de Registro de Preços 040/2021-MP/PA,** e tem como fundamento as Leis Federais nº. 8.078/90 e 8.666/93 e na Lei Estadual nº 5.416/87, observadas as alterações e demais regras de direito público e privado aplicáveis a matéria que o subsidiarem.

1.2. Aos casos omissos serão aplicadas as normas referidas no subitem anterior.

CLÁUSULA SEGUNDA - DO OBJETO

2.1 O presente Contrato tem por objeto a **aquisição de ativos de segurança de rede, Firewalls Next Generation (NGFW) com SD-WAN integrada, contemplando os serviços de Suporte Técnico**, solicitado no protocolo nº **13284/2021,** nas quantidades informadas na cláusula quarta.

CLÁUSULA TERCEIRA - ESPECIFICAÇÃO DETALHADA DOS EQUIPAMENTOS E LICENÇAS

3.1. DESCRIÇÃO

3.1.1. Aquisição de solução de proteção de rede com características de Firewall Next Generation (NGFW) com SD-WAN integrada do tipo Appliance. A solução deve ser integralmente do mesmo fabricante, contemplando gerência centralizada, todos os softwares e suas licenças de uso, possibilitando atualização contínua. Deve incluir, além das funcionalidades citadas acima: Otimização de WAN, gerenciamento centralizada, zero-touch deployment, 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 à internet compondo uma plataforma de segurança integrada e robusta. Na qual todos os links WANs e VPNs devem funcionar simultaneamente;

3.1.2. Por plataforma de segurança entende-se hardware e software integrados do tipo appliance com todas as licenças necessárias inclusas, o sistema operacional fornecido deve ser a versão mais nova disponível, devendo, entretanto, ser considerada estável pelo fabricante do equipamento;

3.1.3. A solução de NGFW deverá suportar mecanismos de redundância de dispositivos em modo ativo-passivo e ativo-ativo, em caso de falha de um dos equipamentos;

3.1.4. Deve possuir LEDs indicadores de status, atividade de rede, status dos links e alimentação;

3.1.5. O equipamento ofertado deve ser compatível com as seguintes funcionalidades:

3.1.5.1. Possibilitar a coleta de estatísticas de todo o tráfego que passar pelo firewall;

3.1.5.2. A solução deve apresentar informações de relatório de acordo com um intervalo de tempo definido pelo administrador;

3.1.5.3. A solução deve contemplar gerenciamento centralizado e integrado de todos os dispositivos da sede e filiais, que possibilite que as configurações, controle de acesso, regras e políticas sejam executadas em um único ponto e replicadas para todos os dispositivos, grupos de dispositivos, usuários, grupos de usuários;

3.1.5.4. O equipamento deve permitir a gestão e monitoramento através da interface de gestão WEB no mesmo dispositivo de proteção da rede;

3.1.5.5. Permitir controle global e centralizado de políticas para todos os equipamentos que compõe a plataforma de segurança;

3.1.5.6. Exportar backup de configuração automaticamente via agendamento;

3.1.5.7. Os hardwares e softwares ofertados na composição deste item não devem estar listados como “end-of-sale”, “end-of-support” ou “end-of-life” por seus respectivos fabricantes na data da abertura das propostas. Não serão aceitos equipamentos que entrem em modo End of Support durante a vigência da garantia ou que entre em modo End of Life pelo período de 1 ano após a assinatura do contrato.

3.2. SD-WAN

3.2.1. Deve possuir capacidade para utilizar, pelo menos 3 (três) links de WAN, sendo no mínimo 2 (dois) links simultâneos.

3.2.2. Realizar balanceamento de tráfego de saída entre os links de Wan primários;

3.2.3. Permitir que a escolha do link WAN de saída seja influenciada por regras definidas pelo administrador de rede da CONTRATANTE e dinamicamente. As regras devem permitir ao menos um dos parâmetros a seguir ou combinação destes:

3.2.4. Endereço IP de origem e/ou destino;

3.2.5. Subredes de origem e/ou destino;

3.2.6. Métricas de Jitter, latência e perda de pacotes por aplicação;

3.2.7. Status da porta de WAN primários (UP ou DOWN);

3.2.8. Toda a comunicação Wan deve trafegar em um túnel VPN ponto-a-ponto estabelecido dinamicamente entre os PONTOS DE PRESENÇA da CONTRATANTE;

3.2.9. Suportar o protocolo de tunelamento GRE (General Routing Encapsulation - RFC 2784);

3.2.10. A solução deve ter um tempo máximo de failover e failback de 300 segundos;

3.2.11. A topologia da rede WAN deve ser dentre outras possíveis, a de malha completa (full mesh);

3.2.12. O estabelecimento do túnel VPN entre os PONTOS DE PRESENÇA pode inicialmente ser orientado pelo concentrador, mas o trafego de dados após o estabelecimento do túnel deve ser realizado diretamente entre os integrantes do túnel, sem consumir throughput do concentrador;

3.2.13. A solução de SD-WAN deverá ser integrada no próprio appliance de NGFW, não sendo aceito quaisquer componentes adicionais com esta função.

CARACTERISTICAS GERAIS

3.3. Por cada equipamento que compõe a plataforma de segurança, entende-se o hardware e as licenças de softwares necessárias para o seu funcionamento;

3.4. Na data da proposta, nenhum dos modelos ofertados poderão estar listados como “*end-of-sale*”, “*end-of-support*” ou “*end-of-life*” por seus respectivos fabricantes. Não serão aceitos equipamentos que entrem em modo *End of Support* durante a vigência da garantia ou que entre em modo *End of Life* pelo período de 1 ano após a assinatura do contrato;

3.5. A solução deve consistir do *appliance* de proteção de rede com funcionalidades de Next *Generation Firewall* (NGFW) e SD-WAN, além de Solução de Gerência Centralizada com Sistema de Armazenamento de Log e Relatórios Centralizados;

3.6. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;

3.7. As funcionalidades de proteção de rede (Firewall, IPS, Antivírus, Filtro Web, Controle de aplicações) que compõem a plataforma de segurança, devem funcionar localmente nos dispositivos NGFW;

3.8. A funcionalidade de *Sandbox* deve ser executada em nuvem pelo próprio fabricante, devendo o NGFW estar devidamente licenciado para possibilitar a execução desta função;

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

3.10. O hardware e software que executa as funcionalidades de proteção de rede firewall (NGFW) e SD-WAN deve ser do tipo *appliance*. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;

3.11. Os *appliances* que executarão a função de NGFW deverão ter altura máxima de 1 (um) U de espaço em rack;

3.12. O software deverá ser fornecido em sua versão mais atualizada e estável;

3.13. Os equipamentos deverão ser fornecidos de acordo com as características técnicas mínimas presentes neste Termo de Referência;

3.14. A solução deverá ser capaz de fechar túneis VPN do tipo IPSec com equipamentos de terceiros (Palo Alto Networks, Cisco, Check Point, Juniper, Fortinet, SonicWall);

3.15. Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:

3.15.1. Suporte a 4094 VLAN Tags 802.1q;

3.15.2. Agregação de links 802.3ad e LACP;

3.15.3. Policy based routing ou policy based forwarding;

3.15.4. Roteamento multicast (PIM-SM e PIM-DM);

3.15.5. DHCP Relay;

3.15.6. DHCP Server;

3.15.7. Jumbo Frames;

3.16. Os dispositivos de proteção de rede devem suportar *sFlow*;

3.17. Suportar sub-interfaces ethernet logicas.

3.18. Deve suportar os seguintes tipos de NAT:

3.18.1. Nat dinâmico (Many-to-1);

3.18.2. Nat dinâmico (Many-to-Many);

3.18.3. Nat estático (1-to-1);

3.18.4. NAT estático (Many-to-Many);

3.18.5. Nat estático bidirecional 1-to-1;

3.18.6. Tradução de porta (PAT);

3.18.7. NAT de Origem;

3.18.8. NAT de Destino;

3.18.9. Suportar NAT de Origem e NAT de Destino simultaneamente.

3.18.10. Deve implementar Network Prefix Translation (NPTv6), prevenindo problemas de roteamento assimétrico;

3.18.11. Deve implementar o protocolo ECMP;

3.18.12. Portas UDP, uma ou um range;

3.18.13. Portas TCP, uma ou um range;

3.18.14. Deve implementar balanceamento de link por hash do IP de origem;

3.18.15. Deve implementar balanceamento de link por hash do IP de origem e destino;

3.18.16. Deve implementar balanceamento de link através do método round-robin;

3.18.17. 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, três links;

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

3.18.19. Seleção do melhor caminho que o tráfego da sessão leva com base na qualidade do circuito baseado em Latência, Perda "Loss" e Jitter;

3.18.20. A solução deve ser capaz de detectar perda, aumento de latência e jitter de um caminho, quando este começa a degradar a qualidade de uma aplicação. Deslocando o tráfego da aplicação para outro circuito de dado que esteja com melhor desempenho de forma transparente para

os usuários, sem que seja percebido interrupção na continuidade do aplicativo ou dos pacotes perdidos;

3.18.21. Deve implementar balanceamento de link através de políticas por aplicação, conforme regras de negócio;

3.18.22. 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;

3.18.23. Enviar log para sistemas de monitoração externos, simultaneamente;

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

3.18.25. Deve permitir configurar certificado caso necessário para autenticação no sistema de monitoração externo de logs;

3.18.26. Proteção contra anti-spoofing;

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

3.18.28. 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;

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

3.18.30. Para IPv6, deve suportar roteamento estático e dinâmico (RIPv6, BGP4+, OSPFv3);

3.18.31. Suportar a OSPF graceful restart;

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

3.18.33. 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);

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

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

3.18.36. 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;

3.18.37. Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;

3.18.38. Suporte à configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo:

3.18.39. Em modo transparente;

3.18.40. Em Layer 3;

3.18.41. A configuração em alta disponibilidade deve sincronizar:

3.18.42. Sessões;

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

3.18.44. Certificados de-criptografados;

3.18.45. Associações de Segurança das VPNs;

3.18.46. Sincronizar tabelas FIB;

3.18.47. HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link;

O gerenciamento da solução deve suportar acesso via SSH e interface WEB (HTTPS), incluindo, mas não limitado à, exportar configuração dos sistemas virtuais (contextos) por ambas interfaces;

3.18.48. As funcionalidades de NGFW e SD-WAN, 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.

3.19. CONTROLE POR POLÍTICA DE FIREWALL

3.19.1. Deverá suportar controles por zona de segurança;

3.19.2. O Firewall deverá possuir controles de segurança de camada L4 - L7;

3.19.3. A solução de firewall deve atuar na camada de aplicação possibilitando ao administrador criar regrar e impedir a utilização de aplicações (*deep packet inspection*);

3.19.4. Controles de políticas por porta e protocolo;

3.19.5. Controle de políticas por aplicações grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;

3.19.6. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;

3.19.7. 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;

3.19.8. Controle de políticas por código de País ou geolocalização (Por exemplo: BR, USA, UK, RUS);

3.19.9. Controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (*Inbound*) e Saída (*Outbound*).

3.19.10. Deve suportar *offload* de certificado em inspeção de conexões SSL de entrada (*Inbound*);

3.19.11. Deve de-criptografar tráfego *Inbound* e *Outbound* em conexões negociadas com TLS 1.2;

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

3.19.13. A 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;

3.19.14. 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);

3.19.15. Bloqueios dos seguintes tipos de arquivos: bat, cab, dll, exe, pif e reg;

3.19.16. *Traffic shaping* QoS baseado em Políticas (Prioridade, Garantia e Máximo);

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

3.19.18. Suporte a objetos e regras IPV6;

3.19.19. Suporte a objetos e regras *multicast*;

3.19.20. Deve possibilitar a utilização de no mínimo 04 ações nas regras de controle como Permitir, Bloquear;

3.19.21. Deve suportar no mínimo os seguintes tipos de negação de tráfego nas políticas de firewall: *Drop* sem notificação do bloqueio ao usuário e TCP-Reset para o cliente;

3.19.22. Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;

3.19.23. O controle por políticas de firewall deverá ser integrado no próprio *appliance* de NGFW, não sendo aceito quaisquer componentes adicionais com esta função.

3.20. CONTROLE DE APLICAÇÕES

3.20.1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;

3.20.2. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;

3.20.3. Reconhecer pelo menos 2000 (duas mil) 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;

3.20.4. 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, onedrive, 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;

3.20.5. Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações customizadas e não somente sobre aplicações conhecidas;

3.20.6. 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;

3.20.7. 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;

3.20.8. 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;

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

3.20.10. 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;

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

3.20.12. Atualizar a base de assinaturas de aplicações automaticamente;

3.20.13. Reconhecer aplicações em IPv6;

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

3.20.15. 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;

3.20.16. 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;

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

3.20.18. 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;

3.20.19. 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, SMTP, Telnet, SSH, MS-SQL, IMAP, MS-RPC e RTSP.

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

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

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

3.20.23. Deve possibilitar a diferenciação de tráfegos para as seguintes aplicações e respectivas granularidades: Instagram (login, post, vídeo, upload de arquivo), YouTube (canais, streaming HD, pesquisa de vídeo, play vídeo), Facebook (upload e download de arquivos, login, chat, botão de like, chamadas VoIP, play vídeo, post, mensagem de voz), WhatsApp (transferência de arquivos, chamadas VoIP e whatsapp web);

3.20.24. Deve possibilitar a diferenciação de aplicações Proxies, possuindo granularidade de controle/políticas para os mesmos;

3.20.25. Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como: Tecnologia utilizada nas aplicações (Client-Server, Browser Based, Network Protocol, etc); Nível de risco da aplicação; Categoria de aplicações;

3.20.26.Deve ser possível configurar *Application Override* permitindo selecionar aplicações individualmente;

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

3.20.28.O controle de aplicações deverá ser integrado no próprio *appliance* de NGFW, não sendo aceito quaisquer componentes adicionais com esta função.

3.21. PREVENÇÃO DE AMEAÇAS

3.21.1. Para proteção do ambiente de redes contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio *appliance* de Firewall;

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

3.21.3. 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;

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

3.21.5. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS, *Anti-Spyware* e Antivírus: permitir, permitir e gerar log, bloquear, e enviar tcp-reset;

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

3.21.7. 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;

3.21.8. Deve permitir o bloqueio de vulnerabilidades;

3.21.9. Deve permitir o bloqueio de *exploits* conhecidos;

3.21.10.Deve incluir proteção contra ataques de negação de serviços;

3.21.11.Fornecem proteção contra ataques de dia zero;

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

3.21.13.Análise de padrões de estado de conexões;

3.21.14.Análise de decodificação de protocolo;

3.21.15.Análise para detecção de anomalias de protocolo;

3.21.16.Análise heurística;

3.21.17.IP *Defragmentation*;

3.21.18.Remontagem de pacotes de TCP.

3.21.19.Bloqueio de pacotes malformados.

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

3.21.21.Detectar e bloquear a origem de portscans;

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

3.21.23.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;

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

3.21.25.Possuir assinaturas para bloqueio de ataques de *buffer overflow*;

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

3.21.27.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;

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

3.21.29.Suportar bloqueio de arquivos por tipo;

3.21.30.Identificar e bloquear comunicação com *botnets*;

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

3.21.32.Deve suportar referência cruzada com CVE;

3.21.33.Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:

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

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

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

3.21.36.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;

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

3.21.38. Deve incluir proteção contra vírus em conteúdo HTML e Java script, software espião (Spyware) e worms;

3.21.39.Proteção contra downloads involuntários usando HTTP de arquivos executáveis;

3.21.40.Rastreamento de vírus em pdf;

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

3.21.42.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.

3.21.43.A prevenção de ameaças deverá ser integrada no próprio appliance de NGFW, não sendo aceito quaisquer componentes adicionais com esta função.

3.22. ANÁLISE DE MALWARE

3.22.1. 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 dever possuir funcionalidades para análise de Malwares não conhecidos incluídas na própria ferramenta ou entregue com composição com outro fabricante sem custo adicional;

3.22.2. 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;

3.22.3. 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;

3.22.4. Deve possuir a capacidade de diferenciar arquivos analisados em pelo menos três categorias: malicioso, não malicioso e suspeito;

3.22.5. Suportar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Android, MacOS, Windows 8, Windows 7 (32 bits) e Windows 7 (64 bits), Windows 10 (32 bits) e Windows 10 (64 bits);

3.22.6. 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;

3.22.7. 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;

3.22.8. O sistema de análise "*In Cloud*" ou local deve 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*);

3.22.9. Caso a solução seja fornecida em *appliance* local, deve possuir, no mínimo, 28 ambientes controlados (*Sandbox*) independentes para execução simultânea de arquivos suspeitos;

3.22.10.Caso seja necessário, licenças de sistemas operacional e softwares para execução de arquivos no ambiente controlado (*Sandbox*), as mesmas devem ser fornecidas em sua totalidade, sem custos adicionais para a contratante;

3.22.11.Suportar a análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL no ambiente controlado;

3.22.12.Deve atualizar a base com assinaturas para bloqueio dos malwares identificados em Sandbox com frequência;

3.22.13.A análise de Malware deverá ser integrada no próprio appliance de NGFW, não sendo aceito quaisquer componentes adicionais com esta função.

3.23. FILTRO URL

3.23.1. 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);

3.23.2. Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, Ips, Redes e Zonas de segurança;

3.23.3. Incluir nativamente *Explicit Web Proxy* e *proxy Web* transparente;

3.23.4. 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*, base de dados local, inclusive em modo de proxy transparente e explicito;

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

3.23.6. Suporta a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;

3.23.7. Deve bloquear o acesso a sites de busca (Google, Bing e Yahoo). O Firewall deve ter mecanismo que implemente a navegação com o uso o *Safe Search*, independente da intervenção do usuário.

3.23.8. Suporta base ou cache de URLs local no *appliance*, evitando *delay* de comunicação/validação das URLs;

3.23.9. Possui pelo menos 60 categorias de URLs;

3.23.10.A categorização de URL deve analisar toda a URL e não somente até o nível de diretório;

3.23.11.Suporta a criação categorias de URLs customizadas;

3.23.12.Suporta a criação de exceções nos bloqueios de filtro de URLs;

3.23.13.Permite a customização de página de bloqueio;

3.23.14.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);

3.23.15.A funcionalidade de Filtro de URL, categorizada localmente, deve 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;

3.23.16.Suporta a inclusão nos logs do produto de informações das atividades dos usuários;

3.23.17.Deve possuir base ou cache de URLs local no *appliance* ou em nuvem do próprio fabricante, evitando *delay* de comunicação/validação das URLs;

3.23.18.Deve salvar nos logs as informações dos seguintes campos do cabeçalho HTTP nos acessos a URLs: UserAgent, Referer, e X-Forwarded For;

3.24. IDENTIFICAÇÃO DE USUÁRIOS

3.24.1. 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 base de dados local;

3.24.2. Deve possuir integração com Microsoft *Active Directory* e LDAP para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários;

3.24.3. Deve possuir integração com *Radius* para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários;

3.24.4. 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*);

3.24.5. Suporte a autenticação *Kerberos*;

3.24.6. Deve possuir suporte a identificação de múltiplos usuários conectados em 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;

3.24.7. Deve identificar usuários através de leitura do campo nos logs do firewall o endereço IP, bem como o usuário de rede responsável pelo acesso;

3.24.8. Deve permitir a criação de políticas de segurança baseadas em usuários de rede com reconhecimento dos mesmos através de leitura do campo de identificação do usuário;

3.24.9. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;

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

3.25. QOS

3.25.1. 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;

3.25.2. Suportar a criação de políticas de QoS e traffic-shaping por:

3.25.2.1. Endereço de origem;

3.25.2.2. Endereço de destino;

3.25.2.3. Por usuário e grupo do LDAP/AD;

3.25.2.4. Por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;

3.25.2.5. Por porta.

3.25.3. QoS deve possibilitar a definição de classes por:

3.25.3.1. Banda Garantida;

3.25.3.2. Banda Máxima;

3.25.3.3. Fila de Prioridade.

3.25.4. Suportar priorização Real Time de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype;

3.25.5. Suportar marcação de pacotes *Diffserv*, inclusive por aplicação;

3.25.6. Deve implementar QoS (*traffic-shaping*), 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*);

3.25.7. Disponibilizar estatísticas Real Time para classes de QoS;

3.25.8. Deve suportar QoS (*traffic-shaping*), em interface agregadas;

3.25.9. Deverá permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário.

3.26. FILTRO DE DADOS

3.26.1. Permite a criação de filtros para arquivos e dados pré-definidos;

3.26.2. Os arquivos devem ser identificados por extensão, tipo e assinaturas (ou *fingerprint*);

3.26.3. Permite identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, SMTP, POP3, IMAP, MAPI, FTP e NNTP);

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

3.26.5. 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.

3.27. GEOLOCALIZAÇÃO

3.27.1. Suportar a criação de políticas por geolocalização, permitindo o trafego de determinado Pais/Países sejam bloqueados;

3.27.2. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;

3.27.3. Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas.

3.28. VPN

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

3.28.2. Suportar IPSec VPN;

3.28.3. Suportar SSL VPN;

3.28.4. A VPN IPSec deve suportar:

3.28.5. DES e 3DES;

3.28.6. Autenticação MD5 e SHA-1;

3.28.7. Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;

3.28.8. Algoritmo Internet Key Exchange (IKEv1 e v2);

3.28.9. AES 128, 192 e 256 (Advanced Encryption Standard);

3.28.10.Autenticação via certificado IKE PKI.

3.28.11.Deve possuir interoperabilidade com os seguintes fabricantes: Palo Alto Networks, Cisco, Check Point, Juniper, Fortinet, SonicWall;

3.28.12.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;

3.28.13.VPN SSL deve suportar:

3.28.13.1. Usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;

3.28.13.2. A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente. Caso necessite de agente, deve estar licenciada para ou suportar sem o uso de licença, 50 (cinquenta) clientes de VPN SSL simultâneos;

3.28.13.3. Atribuição de endereço IP nos clientes remotos de VPN SSL;

3.28.13.4. Deve permitir a atribuição de IPs fixos nos usuários remotos de VPN SSL.

3.28.14.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;

3.28.15.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;

3.28.16.Atribuição de DNS nos clientes remotos de VPN;

3.28.17.Deve suportar autenticação de clientes VPN a partir de diferentes sistemas operacionais remotos (Android, IOS, Mac Windows e Chrome OS);

3.28.18.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;

3.28.19.Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Anti-Spywares e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;

3.28.20. Suportar autenticação via AD/LDAP, OTP (One Time Password), certificado e base de usuários local;

3.28.21.Suporta leitura e verificação de CRL (certificate revocation list);

3.28.22.Permite a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;

3.28.23.Agente deverá comunicar-se com o portal para determinar as políticas de segurança do usuário;

3.28.24.Deve permitir que a conexão com a VPN SSL seja estabelecida das seguintes formas:

3.28.24.1. Antes do usuário autenticar na estação;

3.28.24.2. Após autenticação do usuário na estação;

3.28.24.3. Sob demanda do usuário.

3.28.25.Deverá manter uma conexão segura com o portal durante a sessão;

3.28.26.O agente de VPN SSL client-to-site deve ser compatível com pelo menos: Windows 7, Windows 8 e Mac Osx.

3.29. COMPATIBILIDADE

3.29.1. Todos os itens de hardware e software fornecidos pela PROPONENTE deverão ser da mesma marca e fabricante. A padronização da marca garante que os equipamentos adquiridos sejam 100% compatíveis entre si, permitindo a proteção de investimento a ser realizado por este órgão. Desta forma, faz-se necessária a aquisição de produtos de mesma marca e fabricante, com o fim de garantir a interoperabilidade e possibilidade de operar em Alta Disponibilidade entre si.

3.30. LICENCIAMENTO

3.30.1. Deve ser fornecido com a versão de software mais recente disponível para o equipamento;

3.30.2. Deve ser fornecido com todas as licenças de software necessárias para o funcionamento de todos os recursos descritos e exigidos neste termo para o prazo mínimo de 05 anos.

3.31. GARANTIA E SUPORTE

3.31.1. Durante o prazo de 05 anos, deve ser possível realizar a atualização de sistema operacional dos equipamentos, incluindo atualizações de novas assinaturas;

3.31.2. 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);

3.31.3. Os chamados poderão ser abertos diretamente com o fabricante ou autorizada pelo fabricante através de ligação telefônica 0800 no idioma Português, bem como via website e/ou e-mail durante a vigência da garantia (5 anos), sendo tais canais de comunicação informados pela CONTRATADA, por ocasião da assinatura da ARP/Contrato, indicando a empresa que prestará os serviços de garantia, com todas as informações necessárias (endereço completo, telefone, fax, e-mail e, se houver, responsável técnico) através de declaração assinada pelo representante legal da mesma, específica para este pregão. A substituição da empresa indicada para a prestação da garantia on-site somente poderá ser feita mediante comunicação e autorização prévia do Ministério Público do Estado do Pará.

3.31.4. 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.

3.32. DOS ITENS DO LOTE 01

3.32.1. Item 01 - NGFW de pequeno porte com SD-WAN integrada, garantia, suporte e todas as licenças necessárias: 134 (cento e trinta e quatro) unidades.

3.32.1.1. CAPACIDADE E QUANTIDADE

3.32.1.1.1. Throughput de, no mínimo, 02 (dois) Gbps com a funcionalidade de firewall habilitada;

3.32.1.1.2. Throughput de no mínimo 450 (quatrocentos e cinquenta) Mbps com a funcionalidade de controle de aplicação e logs habilitada;

3.32.1.1.3. Throughput de no mínimo 160 (cento e sessenta) Mbps com as seguintes funcionalidades habilitadas: controle de aplicação, IPS, Antivírus e Anti-Spyware e log. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, todas deverão ter valor superior ao throughput requerido;

3.32.1.1.4. Capacidades (throughput) comprovadas por documento de domínio público disponibilizado pelo fabricante, não sendo admitida 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;

3.32.1.1.5. Efetividade de Segurança mínima de 80%, classificados como recomendado em Security Value Map (SVM) Comparative Report para Next Generation Firewall (NGFW) da NSSLabs ou certificação ICSA Labs para o ano de 2018 ou posterior, seja para o modelo apresentado ou para equipamento da mesma linha que possua mesmo sistema operacional e engine de anti-vírus, comprovada por documento de domínio público;

3.32.1.1.6. Suporte a, no mínimo, 192 (Cento e noventa e dois) mil conexões simultâneas;

3.32.1.1.7. Suporte a, no mínimo, 13 (treze) mil novas conexões por segundo;

3.32.1.1.8. Fonte de alimentação automática 100-240V AC;

3.32.1.1.9. Possuir espaço em disco SSD interno com no mínimo 32 (trinta e dois) GB;

3.32.1.1.10. No mínimo 7 (sete) interfaces de rede gigabit Ethernet RJ45, devendo ser possível configurar ao menos 02 (duas) destas interfaces como WAN;

3.32.1.1.11. 01 (uma) interface do tipo console ou similar;

3.32.1.1.12. Suporte a, no mínimo, 20 (vinte) zonas de segurança;

3.32.1.1.13. Estar licenciada para suportar sem o uso de licença, 200 (duzentos) clientes de VPN SSL simultâneos;

3.32.1.1.14. Estar licenciada para suportar sem o uso de licença, 200 (duzentos) túneis de VPN IPSEC simultâneos.

3.32.2. Item 02 - NGFW de médio porte com SD-WAN integrada, garantia, suporte e todas as licenças necessárias: 20 (vinte) unidades

3.32.2.1. CAPACIDADE E QUANTIDADE

3.32.2.1.1. Throughput de, no mínimo, 10 (dez) Gbps com a funcionalidade de firewall habilitada;

3.32.2.1.2. Throughput de no mínimo 02 (dois) Gbps com a funcionalidade de controle de aplicação e logs habilitada;

3.32.2.1.3. Throughput de no mínimo 700 (setecentos) Mbps com as seguintes funcionalidades habilitadas simultaneamente: controle de aplicação IPS, Antivírus e Anti-Spyware e logs. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, todas deverão ter valor superior ao throughput requerido;

3.32.2.1.4. Capacidades (throughput) comprovadas por documento de domínio público disponibilizado pelo fabricante, não sendo admitida 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;

3.32.2.1.5. Efetividade de Segurança mínima de 80%, classificados como recomendado em Security Value Map (SVM) Comparative Report para Next Generation Firewall (NGFW) da NSSLabs ou certificação ICSA Labs para o ano de 2018 ou posterior, seja para o modelo apresentado ou para equipamento da mesma linha que possua mesmo sistema operacional e engine de anti-vírus, comprovada por documento de domínio público; Suporte a, no mínimo, 1,5 (um vírgula cinco) milhão de conexões simultâneas;

3.32.2.1.6. Suporte a, no mínimo, 50 (cinquenta) mil novas conexões por segundo;

3.32.2.1.7. Fonte de alimentação automática 100-240V AC;

3.32.2.1.8. Possuir espaço em disco SSD interno com no mínimo 240 (duzentos e quarenta) GB;

3.32.2.1.9. No mínimo 10 (dez) interfaces de rede gigabit Ethernet RJ45, devendo ser possível configurar ao menos 02 (duas) destas interfaces como WAN;

3.32.2.1.10. No mínimo 08 (oito) slots SFP;

3.32.2.1.11. No mínimo 02 (dois) slots SFP+;

3.32.2.1.12. 01 (uma) interface do tipo console ou similar;

3.32.2.1.13. Fonte de alimentação automática 100-240V AC;

3.32.2.1.14. Suporte a, no mínimo, 06 (seis) sistemas virtuais lógicos (Contextos) no firewall físico. Os contextos virtuais devem suportar as funcionalidades nativas do gateway de proteção incluindo: Firewall, IPS, Antivírus, Anti-Spyware, Filtro de URL, Filtro de Dados, VPN, Controle de Aplicações, QoS, NAT e Identificação de usuários;

3.32.2.1.15. Suporte a, no mínimo, 50 (cinquenta) zonas de segurança;

3.32.2.1.16. Estar licenciada para ou suportar sem o uso de licença, 400 (quatrocentos) clientes de VPN SSL simultâneos;

3.32.2.1.17. Estar licenciada para ou suportar sem o uso de licença, 02 (dois) mil túneis de VPN IPSEC simultâneos.

CLÁUSULA QUARTA - DO PREÇO, DA QUANTIDADE E DOS RECURSOS FINANCEIROS

4.1. O valor global do presente contrato é de **R$ 3.454.484.86 (três milhões, quatrocentos e cinquenta e quatro mil, quatrocentos e oitenta e quatro reais e oitenta e seis centavos)**, conforme o disposto na proposta da Contratada, datada de **09/03/2021**, pela execução do objeto, nas especificações, quantidade e preços unitários abaixo:

Item	Descrição	Und	Qtd	Preço Unitário	Preço Total do item
1	**Marca: Fortinet - Fabricante :Fortinet** NGFW de pequeno porte com SD-WAN integrada, garantia, suporte e todas as licenças necessáriaspara atender a demanda do MPPA.Contempla também todos os acessórios, como Kit para instalação em rack, cabos de energia e cabos console, além de licenciamento de 60 meses do tipo UTP (FC-10-0061F-950-02-60), que contempla serviço de suporte e garantia 24x7, atualização de assinaturas de Controle de Aplicação, IPS, Antivirus, Filtro Web, Antispam, e FortiSandboxCloud. **Modelo: FortiGate 61F (FG-61F)**	UNID	79	R$ 31.519,14	R$ 2.490.012,06
2	**Marca: Fortinet - Fabricante: Fortinet** **NGFW de médio porte** com SD-WAN integrada,garantia, suporte e todas as licenças necessárias para atender a demanda do MPPA. Contempla também todos os acessórios, como Kit para instalação em rack, cabos de energia e cabos console, além de licenciamento de 60 meses do tipo UTP (FC-10-F101F-950-02-60), que contempla serviço de suporte e garantia 24x7, atualização de assinaturas de Controle de Aplicação, IPS, Antivirus, Filtro Web, Antispam, e FortiSandboxCloud. **Modelo: FortiGate 101F (FG-101F)**	UNID	08	R$ 120.559,10	R$ 964.472,80

Parágrafo Único – No valor estabelecido nesta cláusula estão incluídos todos os tributos, contribuições fiscais e parafiscais previstos na legislação em vigor incidentes, direta ou indiretamente e despesas de quaisquer natureza decorrentes da execução do presente contrato.

4.2. Para atender às despesas do presente Contrato, o Ministério Público, valer-se-á de recursos orçamentários na função programática:

Classificação: 12101.03.122.1494.8760 – Governança e Gestão
Elemento: 4490-52 – Equipamentos e Material Permanente
Fonte: 0101 – Recursos Ordinários

CLÁUSULA QUINTA - DAS CONDIÇÕES DE PAGAMENTO

5.1. O pagamento será efetuado pelo Departamento Financeiro do Ministério Público no prazo máximo de **30 (trinta) dias** corridos, no **Banco: Bradesco – 237, Agência n° 6349, Conta Corrente n° 000.1856-2**, salvo atraso na liberação de recursos pela Secretaria Executiva de Planejamento, Orçamento e Finanças - SEPOF, após o recebimento definitivo da solução e dos serviços licitados, mediante a apresentação das Notas Fiscais devidamente atestadas pelo FISCAL, o qual observará as especificações exigidas.

5.1.1. O pagamento dos fornecedores de bens e prestadores de serviços dos órgãos da Administração Direta e Indireta do Estado do Pará será efetuado mediante crédito em conta corrente aberta no Banco do Estado do Pará S/A – BANPARÁ, conforme Decreto Estadual nº 877, de 31/03/2008.

5.1.2. Caso o prestador não possua conta no banco BANPARÁ, será cobrada pelo banco taxa referente ao DOC/TED, sendo o valor desta taxa automaticamente descontado no valor depositado para pagamento da prestação do serviço**.**

5.1.3. Pagamentos através de código de barra só poderão ser realizados caso a empresa possua convênio com o Banco do Estado do Pará (BANPARÁ), uma vez que todos os pagamentos são realizados através do SIAFEM (Sistema Integrado de Administração Financeira de Estados e Municípios).

5.2. O atesto da nota fiscal será efetuado no prazo máximo de 05 (cinco) dias úteis contados do recebimento definitivo do material pelo responsável pela Fiscalização no local anteriormente mencionado;

5.3. A nota fiscal que contiver erro será devolvida à contratada para retificação e reapresentação, iniciando a contagem dos prazos fixados para o ATESTO a partir do recebimento da Nota Fiscal corrigida.

5.4. A CONTRATADA deverá encaminhar, junto com a nota fiscal, os seguintes documentos:

5.4.1. Certidão conjunta negativa de débitos relativos aos tributos federais e a dívida ativa da União;

5.4.2. Certidão negativa de débitos relativos às Contribuições Previdenciárias;

5.4.3. Certificado de regularidade do FGTS – CRF;

5.4.4. Certidão negativa de débitos inadimplidos perante a Justiça do Trabalho;

5.4.5. Certidão negativa de débitos com Fazenda Estadual;

5.4.6. Certidão negativa de débitos com a Fazenda Municipal;

5.5. Ocorrendo erro no documento da cobrança, este será devolvido e o pagamento será sustado para que a CONTRATADA tome medidas necessárias, passando o prazo para o pagamento a ser contado a partir da data da reapresentação do mesmo.

5.6. Não efetuado o pagamento pelo CONTRATANTE no prazo estabelecido na sub-cláusula 5.1, e desde que não haja culpa da CONTRATADA, os valores correspondentes à fatura serão atualizados financeiramente com base no critério abaixo especificado, em observância ao art. 40, XIV, “c” da Lei 8.666/93 e suas alterações.

EM=I x N x VP

Onde:

EM=Encargos Monetários

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

VP=Valor da parcela a ser paga

I=Índice de atualização financeira = 0, 0001644, assim apurado:

$$I = \frac{TX/100}{365} \qquad I = \frac{6/100}{365} \qquad I = 0{,}0001644$$

TX=Percentual da taxa anual=6%

CLÁUSULA SEXTA – DOS ACRÉSCIMOS E SUPRESSÕES E DEMAIS ALTERAÇÕES

6.1. Nos itens a partir de 04 unidades, a contratada fica obrigada a aceitar, nas mesmas condições contratuais, os acréscimos e supressões até 25% (vinte e cinco por cento) do valor inicial atualizado do contrato, referentes à alteração quantitativa do item, nos termos do art. 65, § 1º, da Lei nº. 8.666/93, salvo a exceção prevista no § 2º do referido artigo

6.2. Este instrumento poderá ainda ser alterado, exceto no objeto, nos termos do atr. 65 da Lei 8.66/93 e com as devidas justificativas, nos seguintes casos:

I - Unilateralmente pela Administração:

a) quando houver modificação do projeto ou das especificações, para melhor adequação técnica aos seus objetivos;

b) quando necessária a modificação do valor contratual em decorrência de acréscimo ou diminuição quantitativa de seu objeto, nos limites permitidos por esta Lei;

II - Por acordo das partes:

a) quando conveniente a substituição da garantia de execução;

b) quando necessária a modificação do regime de execução da obra ou serviço, bem como do modo de fornecimento, em face de verificação técnica da inaplicabilidade dos termos contratuais originários;

c) quando necessária a modificação da forma de pagamento, por imposição de circunstâncias supervenientes, mantido o valor inicial atualizado, vedada a antecipação do

pagamento, com relação ao cronograma financeiro fixado, sem a correspondente contraprestação de fornecimento de bens ou execução de obra ou serviço;

d) para restabelecer a relação que as partes pactuaram inicialmente entre os encargos do contratado e a retribuição da administração para a justa remuneração da obra, serviço ou fornecimento, objetivando a manutenção do equilíbrio econômico-financeiro inicial do contrato, na hipótese de sobrevirem fatos imprevisíveis, ou previsíveis porém de consequências incalculáveis, retardadores ou impeditivos da execução do ajustado, ou, ainda, em caso de força maior, caso fortuito ou fato do príncipe, configurando álea econômica extraordinária e extracontratual.

CLÁUSULA SÉTIMA – DO REAJUSTE

7.1. O valor proposto e contratado poderá ser reajustado, em consonância com as disposições desta Cláusula.

7.1.1. Caso assim queira, a contratada deverá requerer o reajustamento do preço, mediante protocolo no Ministério Público do Estado do Pará, até a data em que se completar cada período de 12 (doze) meses de vigência do contrato, sob pena de preclusão quanto ao período correspondente.

7.1.2. A data-base para o cálculo do reajuste é a data da apresentação da proposta.

7.1.3. Para o cálculo do reajuste, deverá ser adotado o IGP-DI (da Fundação Getúlio Vargas), em sua variação para o período de 12 (doze) meses, a contar da data-base referida no item 7.1.2.

7.1.4. O valor reajustado será concedido somente a partir da data de cada prorrogação, ainda que posterior à anualidade da proposta, e observados os itens anteriores.

7.2. Se a contratada requerer o reajustamento do preço em conformidade com o item 7.1.1, mas o valor reajustado ainda não puder ser concedido na data da prorrogação contratual, por indisponibilidade do índice para a variação referida no item 7.1.3, constará do termo aditivo de prorrogação a ressalva do direito da contratada ao reajuste do preço, que ocorrerá efetivamente mediante termo aditivo específico e quando houver aquela disponibilidade, com retroatividade à data de cada prorrogação.

7.3. Não serão admitidos requerimentos de reajustes para períodos preclusos

CLÁUSULA OITAVA - DOS PRAZOS E CONDIÇÕES DE ENTREGA, RECEBIMENTO E GARANTIA

8.1. CONTRATADA se compromete a efetuar a entrega dos produtos solicitados no prazo não superior a 60 (sessenta) dias corridos, a contar do início da vigência do contrato**.**

8.2. A entrega dos produtos será no Edifício Sede do Ministério Público, sito na Rua João Diogo, n. 100 – 2º andar, Cidade Velha, Belém, Pará, no horário das 08h00min às 14h00min, de segunda a sexta-feira, exceto nos feriados e dias facultativos, correndo por conta da contratada todas as despesas de embalagem, seguros, transporte, tributos, encargos trabalhistas e previdenciários, decorrentes do serviço e equipamentos necessários para o seu funcionamento, devendo a entrega ser agendada, com até 48h de antecedência, pelos telefones (91) 4006-3480/3481;

8.3. O CONTRATADO terá prazo de 06 (seis) dias úteis a contar da comunicação para retirar a Nota de Empenho de Despesas ou instrumento equivalente.

8.4. Os equipamentos deverão ser novos (de primeiro uso), e deverão ser entregues devidamente protegidos e adequadamente embalados contra danos de transporte manuseio e acompanhados das notas fiscais de remessa;

8.5. Caso se veja impossibilitada de cumprir com o prazo estipulado no item 4.1, a Contratada deverá, por escrito e com antecedência mínima de 10 (dez) dias corridos antes de expirado o prazo, solicitar prorrogação do prazo e apresentar justificativas;

8.6. O pedido de prorrogação, com indicação do novo prazo, quando for o caso, deverá ser encaminhado à fiscalização da Contratante, que poderá, de modo justificado, acolher ou não o pedido;

8.7. Vencidos os prazos de entrega ou de prorrogação e não cumprida a obrigação de entrega, a Contratante oficiará a Contratada acerca do transcurso da data limite, passando o inadimplemento, a partir daí, a ser considerado como recusa do cumprimento da obrigação pactuada e, por conseguinte, sujeitando a empresa às penalidades prevista na lei;

8.8. O recebimento do objeto pela FISCALIZAÇÃO ou COMISSÃO DE RECEBIMENTO (nas compras acima de R$ 80.000,00) se dará em duas etapas:

a) Em caráter provisório, imediatamente após a entrega dos equipamentos (item 1 e 2), representada pela conferência da quantidade e da qualidade do material entregue (está em sentido da aparência da embalagem) e conformidade com o modelo indicado na proposta comercial;

b) Definitivamente, em até 10 (dez) dias úteis a contar do recebimento provisório, mediante análise individual, que comprove sua conformidade com os padrões estabelecidos no presente Edital;

c) Os objetos serão recebidos e conferidos pela Fiscalização/Comissão de Recebimento designada por esta Instituição.

8.9. O objeto somente será considerado entregue quando emitido o Termo de Recebimento Definitivo dos Bens pela Contratante;

8.10. Se, após o recebimento provisório, constatar-se que os equipamentos foram entregues em desacordo com o solicitado, fora da especificação ou incompletos, após a notificação à Contratada, será suspenso o pagamento até que sanada a situação, independente de aplicação de sanções cabíveis;

8.11. O recebimento do material não exclui a responsabilidade administrativa, civil e penal da empresa por problemas causados durante o uso dos itens adquiridos nem exclui a responsabilidade da CONTRATADA pelo perfeito desempenho do objeto fornecido, cabendo-lhe sanar quaisquer irregularidades detectadas quando de sua utilização;

8.12. A Contratada e/ou detentora da ata deve promover, às suas expensas, a substituição total ou parcial do objeto que apresentar qualquer irregularidade;

8.13. Em caso de qualquer inconformidade, a Contratada terá prazo máximo de 30 (trinta) dias corridos após notificação emitida pela Contratante para sanar quaisquer pendências encontradas, sob pena de aplicação das sanções cabíveis;

8.14. Na hipótese de ser verificada a impropriedade do material no ato da entrega, o mesmo será imediatamente rejeitado, no todo ou em parte, a critério da FISCALIZAÇÃO responsável pelo recebimento, sendo o fornecedor notificado a proceder à substituição no prazo máximo de 30 (trinta) dias corridos, contados da ciência da rejeição, sendo-lhe, ainda, concedidos 05 (cinco) dias úteis para retirada do material ou parte do que foi rejeitado;

8.15. Os profissionais responsáveis pela implantação da solução e treinamento devem ser certificados pelo fabricante da solução;

8.16. A Contratada deverá promover, às suas expensas, a substituição total ou parcial do objeto que apresentar qualquer irregularidade.

8.17. O prazo de garantia será de, no mínimo, 60 (SESSENTA) meses, contados a partir da data do aceite definitivo. A garantia será prestada on-site na sede do MP/PA.

8.18. Os serviços de garantia e suporte técnicos deverão ser prestados aos equipamentos existentes nas dependências do Departamento de Informática – Edifício Sede do MP/PA, 2º Andar, Rua João Diogo, 100, Cidade Velha, Belém, Pará, CEP 66.015.165, assegurando-se, sem ônus para o CONTRATANTE, a cobertura para defeitos de fabricação, pelo período mínimo de 60 (Sessenta) meses, englobando equipamentos, peças e serviços, contados da data em que ocorrer o recebimento definitivo dos bens;

8.19. Durante a vigência dos serviços, chamados técnicos, sem limite de quantidade, poderão ser abertos, no horário de 00:00 às 23:59 horas, de segunda-feira a domingo, via discagem direta gratuita (linha 0800), ou via sistema próprio, em sítio na Internet, caracterizando a abertura do chamado;

8.20. O suporte técnico, deverão ser mantidas pelo prazo definido nas especificações de cada item;

8.21. Os serviços de Suporte e Garantia do equipamento devem ser em regime de 5x8xNBD, modalidade Next Business Day (próximo dia útil comercial), durante o período mínimo de 60 (sessenta) meses para toda a solução, contados da data em que ocorrer recebimento definitivo dos bens;

8.22. O uso da modalidade remota não afeta de forma alguma a contagem dos prazos estipulados;

8.23. O problema dos equipamentos defeituosos, caso comprovado, deverá ser sanado dentro dos tempos estipulados. Quando não for possível solucionar o problema no prazo estipulado, caso

autorizado após avaliação por representante do Departamento de Informática, deverá ser fornecido outro equipamento de igual configuração ou superior, até resolução definitiva do problema;

8.24. A CONTRATADA, no momento da assinatura do Contrato, deverá fornecer número de telefone e/ou endereço de site na internet da central de atendimento para abertura de chamados;

8.25. Os chamados deverão ser resolvidos em até 3 (três) dias úteis, contados do primeiro dia útil seguinte à abertura do mesmo. Findo o prazo de 3 (três) dias úteis, sem a resolução do problema, deverá a CONTRATADA disponibilizar em até 24 horas equipamento de especificação igual ou superior para operação temporária como substituição do equipamento em conserto, o qual deverá ser avaliada e autorizado por representante do Departamento de Informática, não ultrapassando o prazo máximo de 30 (trinta) dias para a solução definitiva do problema;

8.26. O serviço de garantia será prestado com vistas a manter os equipamentos fornecidos em perfeitas condições de uso, sem qualquer ônus adicional para o Ministério Público do Estado do Pará. Nesse sentido, a garantia deve englobar:

a) A remoção dos vícios apresentados pelos equipamentos, materiais, drivers e outros componentes que sejam disponibilizados pelo fabricante dos equipamentos;

b) Solução de problemas e esclarecimento de dúvidas de configuração e de utilização dos equipamentos;

8.27. Os serviços deverão ocorrer de acordo com instruções a serem dadas pelo Departamento de Informática ou por servidor designado para esse fim. A realização dos serviços previstos, a serem efetuados nas dependências do Ministério Público do Estado do Pará, por funcionário da CONTRATADA, deverá ser acompanhada por profissional designado pelo Departamento de Informática do Ministério Público do Estado do Pará;

8.28. As atividades de prestação de serviços de garantia aos equipamentos deverão ocorrer em dias úteis, no período de 8 (oito) às 14 (quatorze) horas;

8.29. Durante todo o período da prestação de serviços de suporte técnico, a CONTRATADA deverá fornecer ao Contratante um usuário e senha para acesso ao sítio do Fabricante na Internet, onde deverá ser possível acompanhar o licenciamento instalado e, em área própria para o modelo ofertado, recursos para consulta e download de:

8.29.1. Softwares, drivers e firmwares (atualizações e/ou versões completas);

8.29.2. Manuais de usuário e dos equipamentos;

8.29.3. Banco de solução para suporte ao software e hardware instalados de fábrica.

8.30. A CONTRATADA deverá manter controle dos chamados abertos, registrando durante toda a vigência contratual ao menos as seguintes informações: número do chamado, número de série do equipamento, data de abertura do chamado, responsável pela abertura do chamado no MPPA, descrição do chamado, local da prestação dos serviços, peças substituídas, data de fechamento do chamado e responsável pela aprovação do fechamento do chamado no MPPA;

8.31. A CONTRATADA deverá indicar, quando da assinatura do contrato, a empresa que prestará os serviços de garantia, com todas as informações necessárias (endereço completo, telefone, fax, e-mail e, se houver, responsável técnico) através de declaração assinada pelo representante legal da mesma, específica para este pregão. A substituição da empresa indicada para a prestação da garantia on-site somente poderá ser feita mediante comunicação e autorização prévia do Ministério Público do Estado do Pará;

8.32. Durante o período da prestação de serviços de garantia e suporte técnico, devem ser disponibilizados e instalados, sem ônus à Contratante, todas as atualizações de software e firmware para os equipamentos, quando for necessário;

8.33. Todos os equipamentos deverão ser previamente registrados pelo fornecedor junto ao fabricante, em nome da Contratante, caso seja uma exigência para fins de garantia;

8.34. Substituir qualquer equipamento durante o prazo de suporte se, em um período de 6 (seis) meses, ocorrer mais de 3 (três) chamados referentes ao mesmo problema (desde que a causa-raiz do mesmo tenha sido atribuída ao equipamento), ou mais de 5 (cinco) chamados referentes a problemas distintos (desde que a causa-raiz dos mesmos tenha sido atribuída ao equipamento);

8.35. A CONTRATADA deve fornecer opção de abertura de ocorrências através de sistema via WEB e através de telefone. O sistema via web, deve ser protegido por senha, permitir a abertura de ocorrências, geração automática do número da ocorrência e o envio automático de correio eletrônico (e-mails) para o pessoal envolvido. Os atendimentos referentes à instalação, análise de performance e ajuste de configurações serão realizados mediante agendamento prévio entre o pessoal técnico

responsável da CONTRATANTE e da CONTRATADA. Ao término de cada atendimento a CONTRATADA deve gerar relatório descrevendo as atividades realizadas e o tempo gasto para tal, este relatório deve ser aprovado pela CONTRATADA.

8.36. Quando da assinatura do contrato, comprovar **através de documentação do fabricante** que os equipamentos especificados para os itens 01 a 03 são novos e de primeiro uso, e que não estarão fora da linha de produção nos próximos **120 (cento e vinte) dias** após a entrega dos mesmos;

8.37. Caso os produtos entregues não sejam de fabricação nacional, deverá ser apresentada original ou cópia autenticada da Declaração de Importação, emitida pela Receita Federal;

8.38. Relativamente, ao disposto nesta clausula, aplicam-se também, subsidiariamente, no que couber, as disposições da Lei nº 8.078 de 11/09/90 – Código de Defesa do Consumidor;

CLÁUSULA NONA – DA VIGÊNCIA DO CONTRATO

9.1. Este O presente Instrumento terá vigência de **05 (cinco) meses**, contados da data da publicação deste instrumento no Diário Oficial do Estado do Pará, **não podendo ser prorrogado**, salvo se ocorrer qualquer um dos motivos do art. 57 §1º, da lei 8.666/93, que implique a prorrogação dos prazos de execução e, consequentemente, exija a prorrogação da vigência do contrato, observado o caput do mesmo dispositivo legal.

CLÁUSULA DÉCIMA - DOS DIREITOS E DAS OBRIGAÇÕES DO CONTRATANTE

10.1. Sem que a isto limite seus direitos, terá o Ministério Público as seguintes garantias:

10.1.1. Receber o objeto de acordo com o que consta neste instrumento;

10.1.2. Devolver o objeto em desacordo com as especificações exigidas.

10.2. Sem que a isto limite sua responsabilidade, será o Órgão responsável pelos seguintes itens:

10.2.1. Cumprir e fazer cumprir o disposto nas condições deste instrumento;

10.2.2. Cumprir todos os compromissos financeiros assumidos com a CONTRATADA no prazo estipulado;

10.2.3. Proporcionar todas as facilidades, inclusive esclarecimentos atinentes ao objeto, para que a empresa possa cumprir as obrigações dentro das normas e condições da aquisição;

10.2.4. Indicar servidor com competência necessária para proceder o recebimento dos objetos e atestar as Notas Fiscais após a verificação das especificações, qualidade, quantidade e preços pactuados;

10.2.5. Promover, através de seu representante, o acompanhamento e a fiscalização do objeto contratado, sob os aspectos quantitativos e qualitativos, prazos de vigência e entregas, anotando em registro próprio as falhas detectadas e comunicando ao Órgão por escrito as advertências e as ocorrências de quaisquer fatos que, a seu critério, exijam medidas corretivas por parte desta;

10.2.6. Emitir nota de empenho a crédito do fornecedor no valor correspondente à quantidade solicitada;

10.2.7. Acompanhar e fiscalizar a perfeita execução do CONTRATO;

10.2.8. Efetuar o pagamento à CONTRATADA referente à quantia efetivamente entregue e após o cumprimento das formalidades legais, no prazo máximo de 30 (trinta) dias corridos contados do atesto da respectiva nota fiscal do material entregue.

CLÁUSULA DÉCIMA PRIMEIRA - DOS DIREITOS E DAS OBRIGAÇÕES DA CONTRATADA

11.1. Sem que a isto limite suas garantias, a CONTRATADA terá os seguintes direitos:

11.1.1. Receber informações e esclarecimentos necessários ao cumprimento das condições estabelecidas;

11.1.2. Receber o Atesto do recebimento do objeto contratado após verificação das especificações;

11.1.3. Receber formalmente a notificação de ocorrência de irregularidades que a fiscalização identificar na execução do objeto, até para que possa a empresa proceder correções;

11.1.4. Receber o pagamento nas condições estabelecidas neste instrumento.

11.2. Sem que a isto limite sua responsabilidade, será a CONTRATADA responsável pelos seguintes itens:

11.2.1. Cumprir fielmente as obrigações assumidas, conforme as especificações, zelando pela fiel execução, utilizando-se de todos os recursos materiais e humanos necessários;

11.2.2. Fornecer o objeto em estrita conformidade com as especificações e condições exigidas, bem como naquelas resultantes de sua proposta, devendo já estar inclusos nos valores propostos todos os custos, impostos, taxas e demais encargos pertinentes à formação do preço;

11.2.3. Entregar os equipamentos e manuais e os prospectos em português no prazo, local e horário previstos no Contrato, observando rigorosamente as exigências estabelecidas nas especificações e na proposta de preços apresentada pela empresa;

11.2.4. Durante o recebimento, substituir o equipamento não aceito pela Contratante em prazo não superior a 30 (trinta) dias corridos, contados da ciência da rejeição;

11.2.5. Responsabilizar-se pelo ônus de retirada e devolução dos equipamentos para realização de serviços de suporte técnico fora das dependências da Contratante;

11.2.6. A CONTRATADA é obrigada a reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, o objeto desta contratação em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou de materiais empregados;

11.2.7. Arcar com todas as despesas, diretas ou indiretas, decorrentes do cumprimento das obrigações assumidas, responsabilizando-se pelos danos causados diretamente à administração ou a terceiros, decorrentes de sua culpa ou dolo, por ocasião da entrega dos objetos no local indicado, incluindo os possíveis danos causados por transportadoras, sem qualquer ônus ao contratante.

11.2.8. Ser responsável pelos encargos trabalhistas, previdenciários, fiscais e comerciais resultantes da execução; a inadimplência da CONTRATADA, com referência aos encargos estabelecidos neste item não transfere a responsabilidade por seu pagamento à Administração do Ministério Público, nem poderá onerar o objeto desta contratação, razão pela qual a CONTRATADA renuncia expressamente a qualquer vínculo de solidariedade, ativa ou passiva, com o Ministério Público;

11.2.9. Quando da assinatura do contrato, comprovar através de documentação do fabricante que os equipamentos especificados para os itens 01 a 03 são novos e de primeiro uso, e que não estarão fora da linha de produção nos próximos 120 (cento e vinte) dias após a entrega dos mesmos;

11.2.10.Caso os produtos entregues não sejam de fabricação nacional, deverá ser apresentada original ou cópia autenticada da Declaração de Importação, emitida pela Receita Federal;

11.2.11.Prestar todos os esclarecimentos que forem solicitados pelo Ministério Público, durante o prazo de fornecimento, credenciando, junto ao Órgão, um representante para prestar os devidos esclarecimentos e atender as reclamações que porventura surgirem durante a execução;

11.2.12.Manter durante todo o prazo de vigência da relação obrigacional com a Contratante a regularidade com o fisco, com o sistema de seguridade social, com a legislação trabalhista, normas e padrões de proteção ao meio ambiente e cumprimento dos direitos da mulher, inclusive os que protegem a maternidade, sob pena da rescisão contratual, sem direito a indenização conforme preceitua o art. 28, §4° da Constituição do Estado do Pará, assim como todas as leis e posturas federais, estaduais e municipais, vigentes, sendo a única responsável por prejuízos decorrentes de infrações a que houver dado causa.

11.2.13.Quando, por problemas, técnicos os prazos pactuados não puderem ser cumpridos, a CONTRATADA deverá comunicar por escrito ao Órgão até 02 (dois) dias úteis anteriores ao término do prazo, ao qual caberá aceitar ou rejeitar as justificativas;

11.2.14.Manter, durante toda a execução, todas as condições de habilitação e qualificação exigidas no Pregão que sejam compatíveis com as obrigações a serem assumidas:

11.2.14.1. Regularidade Fiscal com a Fazenda Nacional, o Sistema de Seguridade Social e o Fundo de Garantia do Tempo de Serviço – FGTS;

11.2.14.2. Regularidade Fiscal perante as Fazendas Estaduais e Municipais da sede da licitante;

11.2.14.3. Regularidade Trabalhista;

11.2.14.4. Cumprimento do disposto no art. 7º, XXXIII, da Constituição Federal/88 (trabalho de menores de idade, observada a Lei nº 9.854/1999);

11.2.15.Informar o Órgão de qualquer alteração necessária à consolidação dos ajustes decorrentes da execução do objeto, tais como: mudança de endereço, razão social, telefone, fax, dissolução da sociedade, falência e outros;

11.2.16.Assumir inteira responsabilidade técnica e administrativa do objeto ADJUDICADO, não podendo, sob qualquer hipótese, transferir a outras empresas a responsabilidade por problemas de funcionamento;

11.2.17.Respeitar e obedecer às normas fixadas pela Administração da CONTRATANTE;

11.2.18.O inadimplemento das obrigações da CONTRATADA, com referência aos encargos trabalhistas, previdenciários, fiscais e comerciais, resultantes da execução, não transfere à Administração da CONTRATANTE a responsabilidade por seu pagamento, nem pode onerar o objeto deste Termo;

11.2.19.Não transferir a outrem, no todo ou em parte, o objeto do presente, sem prévia e expressa anuência do Ministério Público;

11.2.20.A CONTRATADA é obrigada a reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou de materiais empregados.

11.2.21.Responder por acidentes de que possam ser vítimas seus profissionais e, ainda, por eventuais danos causados no local entrega do objeto, aos servidores da CONTRATANTE, bem como a terceiros, quando praticados, por dolo, negligência, imperícia ou imprudência, diretamente por seus empregados na execução do ajuste, arcando, após regular processo administrativo, com a restauração, substituição ou indenização, conforme o caso, devendo os funcionários da empresa contratada apresentarem documentos (RG e CPF) para que seja providenciada a autorização de acesso aos locais indicados na nota de empenho;

11.2.22.Comunicar imediatamente à Administração, bem como ao responsável pela fiscalização, qualquer anormalidade verificada, inclusive de ordem funcional, para que sejam adotadas as providências de regularização necessárias, em qualquer tempo até o final da garantia;

11.2.23.Quando da prestação do eventual serviço de garantia ao equipamento:

11.2.23.1. Fazer-se representar, no local da prestação do eventual serviço de Garantia, por preposto aceito pela Administração com a atribuição de coordenar e fiscalizar a execução dos serviços e o cumprimento das normas disciplinares, de segurança e legislação pertinentes;

11.2.23.2. Atender prontamente às chamadas e às determinações do representante da Administração da CONTRATANTE com vistas a corrigir defeitos observados nos equipamentos entregues dentro do prazo de garantia;

11.2.23.3. Utilizar pessoal técnico qualificado, devidamente identificado com crachás contendo nome, foto e cargo/função desempenhada nas dependências da CONTRATANTE;

11.2.23.4. Comprovar, quando solicitado, a qualificação técnica dos funcionários que irão atender o MPPA;

11.2.23.5. Assumir a responsabilidade por todas as providências e obrigações estabelecidas na legislação específica de acidentes do trabalho, quando, em ocorrência da espécie, forem vítimas os seus empregados no desempenho dos serviços de Assistência Técnica ou em conexão com eles, ainda que acontecido nas dependências da CONTRATANTE;

11.2.24.Assumir todos os encargos sobre demanda trabalhista, previdenciários, obrigações sociais previstas na legislação social e trabalhista em vigor, cível ou penal, relacionado ao eventual serviço de Garantia, originariamente ou vinculados por prevenção, conexão ou contingência, além de assumir a responsabilidade pelos encargos fiscais e comerciais;

11.2.25.São de responsabilidade da CONTRATADA todas e quaisquer despesas decorrentes de sua atividade;

11.2.26.Observar a Resolução nº 172/2017-CNMP que altera o artigo 3º, caput, da Resolução CNMP nº 37/2009 e VEDA ao Ministério Público a contratação das pessoas jurídicas que tenham em seu quadro societário cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade até o terceiro grau, inclusive, dos membros ocupantes de cargos de direção ou no exercício de funções administrativas, assim como de servidores ocupantes de cargos de direção, chefia e assessoramento vinculados direta ou indiretamente às unidades situadas na linha hierárquica da área encarregada da licitação;

11.2.26.1. A vedação do item 11.2.27 não se aplica às hipóteses nas quais a contratação seja realizada por ramo do Ministério Público diverso daquele ao qual pertence o membro ou servidor gerador da incompatibilidade.

11.2.26.2. A vedação do item 11.2.27 se estende às contratações cujo procedimento licitatório tenha sido deflagrado quando os membros e servidores geradores de

incompatibilidade estavam no exercício dos respectivos cargos e funções, assim como às licitações iniciadas até 6 (seis) meses após a desincompatibilização.

11.2.26.3. A contratação de empresa pertencente a parente de membro ou servidor não abrangido pelas hipóteses expressas de nepotismo poderá ser vedada pelo órgão do Ministério Público competente, quando, no caso concreto, identificar risco potencial de contaminação do processo licitatório.

11.2.27.Aceitar o fato de que as informações obtidas em decorrência da execução do presente Termo deverão ser mantidas em sigilo, não podendo qualquer participante divulgá-las fora do âmbito deste instrumento, exceto se previamente acordado por escrito, ou prevista a sua divulgação.

11.2.28. Observar a VEDAÇÃO de contratação de Empresa que tenha entre seus empregados colocados à disposição do Ministério Público para o exercício de funções de chefia, pessoas que incidam na vedação dos arts. 1º e 2º da **Resolução nº 177/2017-CNMP:**

11.2.28.1. Pessoa que tenha sido condenada em decisão com trânsito em julgado ou proferida por órgão jurisdicional colegiado, nos seguintes casos:

I – atos de improbidade administrativa;

II – crimes:

a) contra a administração pública;

b) contra a incolumidade pública;

c) contra a fé pública;

d) contra o patrimônio;

e) de abuso de autoridade, nos casos em que houver condenação à perda do cargo ou à inabilitação para o exercício de função pública;

f) de tráfico de entorpecentes e drogas afins, racismo, tortura, terrorismo e hediondos;

g) contra a vida e a dignidade sexual;

h) praticados por organização ou associação criminosa;

i) de redução de pessoa à condição análoga à de escravo;

j) eleitorais, para os quais a lei comine pena privativa de liberdade;

k) de lavagem ou ocultação de bens, direitos e valores.

11.2.28.2. Aqueles que tenham:

I – praticado atos causadores da perda do cargo ou emprego público, reconhecidos por decisão transitada em julgado ou proferida por órgão judicial colegiado;

II – sido excluídos do exercício da profissão, por decisão definitiva sancionatória judicial ou administrativa do órgão profissional competente, salvo se o ato houver sido anulado ou suspenso pelo Poder Judiciário;

III – tido suas contas relativas ao exercício de cargos ou funções públicas rejeitadas por irregularidade insanável que configure ato doloso de improbidade administrativa, por decisão irrecorrível do órgão competente, salvo se esta houver sido suspensa ou anulada pelo Poder Judiciário, devendo tal condição constar expressamente dos editais de licitação.

CLÁUSULA DÉCIMA SEGUNDA –DA GARANTIA DE EXECUÇÃO DO CONTRATO (somente para contratos a partir de R$100.000,00)

12.1. A **CONTRATADA** deverá prestar a garantia de execução do contrato, **no valor de R$172.724,24 (cento e setenta e dois mil, setecentos e vinte e quatro reais e vinte e quatro centavos), equivalente a 5% do contrato,** nos moldes do art. 56 da Lei nº 8.666, de 1993, com validade durante a execução do contrato e 90 (noventa) dias após término da vigência contratual, devendo ser renovada a cada prorrogação, observados ainda os seguintes requisitos:

12.1.1. A contratada deverá apresentar, no prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, a critério do órgão contratante, contado da assinatura do contrato, comprovante de prestação de garantia, podendo optar por caução em dinheiro ou títulos da dívida pública, seguro-garantia ou fiança bancária;

12.1.1. A garantia, qualquer que seja a modalidade escolhida, assegurará o pagamento de:

i. Prejuízos advindos do não cumprimento do objeto do contrato;

ii. Prejuízos diretos causados à Administração decorrentes de culpa ou dolo durante a execução do contrato;

iii. Multas moratórias e punitivas aplicadas pela Administração à contratada; e

iv. Obrigações trabalhistas e previdenciárias de qualquer natureza, não adimplidas pela contratada, quando couber.

12.1.2. A modalidade seguro-garantia somente será aceita se contemplar todos os eventos indicados no subitem 12.1.2 acima, observada a legislação que rege a matéria;

12.1.3. A garantia em dinheiro deverá ser efetuada no **Banco do Estado do Pará** em conta específica com correção monetária, em favor do contratante;

12.1.4. A inobservância do prazo fixado para apresentação da garantia acarretará a aplicação de multa de 0,07% (sete centésimos por cento) do valor do contrato por dia de atraso, observado o máximo de 2% (dois por cento);

12.1.5. O atraso superior a 15 (quinze) dias autoriza a Administração a promover a rescisão do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõem os incisos I e II do art. 78 da Lei nº 8.666, de 1993;

12.1.6. O garantidor não é parte para figurar em processo administrativo instaurado pelo contratante com o objetivo de apurar prejuízos e/ou aplicar sanções à contratada;

12.1.7. A garantia será considerada extinta:

i. Com a devolução da apólice, carta-fiança ou autorização para o levantamento de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração da Administração, mediante termo circunstanciado, de que a contratada cumpriu todas as cláusulas do contrato; e

ii. Com o término da vigência do contrato, observado o prazo previsto no subitem 12.1 acima, que poderá, independentemente da sua natureza, ser estendido em caso de ocorrência de sinistro.

12.1.8. O contratante executará a garantia na forma prevista na legislação que rege a matéria;

12.2. O Contratante fica autorizado a utilizar a garantia para corrigir as imperfeições na execução do Objeto deste contrato ou reparar danos decorrentes da ação ou omissão do Contratado ou de preposto seu ou, ainda, para satisfazer qualquer obrigação resultante ou decorrente de suas ações ou omissões.

12.3. O Contratado se obriga a repor, no prazo de 48 (quarenta e oito) horas, o valor da garantia que vier a ser utilizado pelo Contratante.

12.4. Em caso de acréscimo ao valor contratual, por meio de termo aditivo, o Contratado fica obrigado a prestar garantia adicional de 5% sobre o valor acrescido;

12.4.1. A garantia prestada será retida definitivamente, integralmente ou pelo saldo que apresentar, no caso de rescisão por culpa do Contratado, sem prejuízo das penalidades cabíveis.

12.4.2. A garantia será restituída, automaticamente ou por solicitação, somente após integral cumprimento de todas as obrigações contratuais, inclusive recolhimento de multas e satisfação de prejuízos causados ao Contratante.

12.4.3. Em se tratando de modalidade fiança bancária, deverá constar do instrumento a expressa renúncia pelo fiador dos benefícios previstos nos arts. 827 e 835 do Código Civil.

CLÁUSULA DÉCIMA TERCEIRA – DAS PENALIDADES

13.1. Pela inexecução total ou parcial do contrato a Administração poderá, garantida a prévia defesa, aplicar ao contratado as sanções previstas nos art. 86 e 87 da lei 8.666/93, conforme segue:

13.2. ADVERTÊNCIA

13.2.1. Advertência, no caso de descumprimento de Cláusula Contratual que não interfira na execução dos serviços ou na sua conclusão e não traga sérios prejuízos econômicos e funcionais a este Órgão;

13.3. MULTA

13.3.1. De 0,25% ao dia, até o limite máximo de 5%, sobre o valor total **do item solicitado**, nos casos de atraso injustificado nos prazos de **retirada/aceite da nota de empenho**.

13.3.1.1. Após o 20º dia de atraso dos prazos previstos, sem justificativa aceita pela Administração, o objeto será considerado como inexecutado.

13.3.2. De 0,25% ao dia, até o limite máximo de 5%, sobre o valor total **da respectiva nota de empenho**, nos casos de atraso injustificado nos prazos **entrega do objeto; substituição do objeto**.

13.3.2.1. Após o 20º dia de atraso dos prazos previstos, sem justificativa aceita pela Administração, o objeto será considerado como inexecutado.

13.3.3. De 10%, sobre o valor total **do item solicitado**, nos casos de:

I. Recusa injustificada em retirar/aceitar a **nota de empenho**, se configurar inexecução total;

13.3.4. De 10%, sobre o valor total **da respectiva nota de empenho**, nos casos de:

I. Recusa injustificada em **entregar/executar o objeto**, se configurar inexecução total;

II. Recusa injustificada em substituir o objeto recusado ou com vícios, se configurar inexecução total;

III. Outras hipóteses de inexecução total do objeto.

13.3.5. De 10%, sobre o valor total **da respectiva nota de empenho**, nos casos de:

I. Recusa injustificada em retirar/aceitar a nota de empenho, se configurar inexecução parcial;

II. Entregar/executar parcial o objeto;

III. Recusa injustificada em substituir o objeto recusado ou com vícios, se configurar inexecução parcial;

IV. Outras hipóteses de inexecução parcial do objeto.

13.3.6. A inobservância do prazo fixado para apresentação da **garantia de execução do contrato** acarretará a aplicação de multa de 0,07% (sete centésimos por cento) do valor do contrato por dia de atraso, observado o máximo de 2% (dois por cento);

13.3.7. De 5% sobre o valor total **da respectiva nota de empenho** nos casos de irregularidade no cumprimento do objeto ou na prestação da garantia do produto do objeto contratado, não referidas nos itens anteriores

13.3.8. As multas são autônomas e a aplicação de uma não exclui a outra;

13.3.9. Havendo garantia à execução apresentada pela empresa, o valor da multa será descontado da mesma. Não havendo garantia ou caso o valor da multa seja superior à referida, a multa ou a diferença será cobrada administrativamente pela Contratante, podendo ser descontado dos créditos devidos, ou ainda judicialmente.

13.4. SUSPENSÃO

13.4.1. Nos casos de inexecução total ou parcial ou irregularidade não justificada e/ou não aceita pela administração e não previstos no item 28.4.1 do edital, aplicar-se-á Suspensão Temporária de participar em licitação e impedimento de contratar com o Ministério Público do Estado do Pará, pelo período de até 02 (dois) anos, na seguinte graduação:

I. 1 (um) ano, nos casos de inexecução parcial não justificada e/ou não aceita pela Administração ou irregularidade na execução;

II. 2 (dois) anos, nos casos de inexecução total não justificada e/ou não aceita pela Administração.

13.5. DECLARAÇÃO DE INIDONEIDADE

13.5.1. No caso de inexecução do objeto que configure ilícito penal, será declarada a inidoneidade da Contratada para licitar e contratar com a Administração Pública Estadual, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade.

CLÁUSULA DÉCIMA QUARTA – DA RESCISÃO

14.1. O presente Contrato poderá ser rescindido:

14.1.1. Unilateralmente nos casos enumerados nos incisos I a XII e XVII, do Art. 78 da Lei n°. 8.666/93;

14.1.2. Amigavelmente, por acordo entre as partes, reduzida a termo no processo da Licitação;

14.1.3. Judicialmente, nos termos da Legislação Processual.

14.1.4. No caso de rescisão Contratual, devidamente justificada nos autos do Processo, terá o contratado o prazo de 05 (cinco) dias úteis, contados da notificação, para apresentar o contraditório e a ampla defesa.

14.2. A inexecução total ou parcial do contrato enseja a sua rescisão, com as consequências contratuais e as previstas em lei ou regulamento

CLÁUSULA DÉCIMA QUINTA – DA FISCALIZAÇÃO

15.1. Será designado servidor para representar a Administração no exercício do dever de acompanhar e fiscalizar a execução do presente contrato, nos termos do art. 67 da Lei nº 8.666/93.

CLÁUSULA DÉCIMA SEXTA - DA PUBLICAÇÃO

16.1. A publicação do presente Instrumento em extrato, no Diário Oficial do Estado, ficará a cargo do Contratante, no prazo e forma disposto na legislação pertinente.

CLÁUSULA DÉCIMA SÉTIMA - DO FORO

17.1. Fica eleito o foro da Justiça Estadual do Pará, Comarca de Belém, Capital do Estado do Pará, para dirimir quaisquer questões oriundas do presente Contrato.

E por estarem justos, contratados e de comum acordo, assinam o presente em duas vias de igual teor e forma, que declaram haver lido, na presença de duas testemunhas, para que possa produzir seus efeitos legais.

Belém-Pa, 22 de setembro de 2021

PARA MINISTERIO PUBLICO:05054960000158
Assinado de forma digital por PARA MINISTERIO PUBLICO:05054960000158
Dados: 2021.09.22 12:10:22 -03'00'

MINISTÉRIO PÚBLICO DO ESTADO DO PARÁ
Contratante

REYNALDO COSTA E ROSA:90158075587
Assinado de forma digital por REYNALDO COSTA E ROSA:90158075587
Dados: 2021.09.21 17:20:34 -03'00'

SIGMAFONETELECOMUNICAÇÕES LTDA
Contratada

Testemunhas:

1. .....
RG: .....

JOAO WALDEMIRO MALTACA CORDEIRO:06142434910
Assinado de forma digital por JOAO WALDEMIRO MALTACA CORDEIRO:06142434910
Dados: 2021.09.21 17:21:53 -03'00'

2. .....
RG:.....

MICHELLE BARBOSA DE BRITO:67911595291
Assinado de forma digital por MICHELLE BARBOSA DE BRITO:67911595291
Dados: 2021.09.22 12:11:37 -03'00'