TERMO DE REFERÊNCIA

A presente licitação tem por objeto á aquisição de Equipamento de Informática. Conforme o Programa de Estruturação Tecnológica Sede e Inspetorias do CREA-RO 2019 do tipo hardware firewall físico.

Porto Velho-RO
Outubro/2019

TERMO DE REFERÊNCIA

***1. OBJETO*.**

1.1. A presente licitação tem por objeto á Aquisição de Equipamentos de Informática. Conforme o Programa de Estruturação Tecnológica Sede e Inspetorias, condições quantidades e exigências estabelecidas neste termo de referência do tipo de Solução de Firewall Físico (Hardware) com serviços de Next Generation Firewall com recursos/licenciamento **ADVANCED GATEWAY SECURITY SUITE**.

2. DA JUSTIFICATIVA.

Nos últimos anos, a Tecnologia da Informação (TI) cresceu muito rapidamente em capacidade e teve uma drástica redução em custo. Novos produtos emergiam rapidamente e outros já existentes mudaram. A taxa de mudança da TI tem sido estimada em 20 a 30% por ano, com resultado disso, os desafios gerenciais da TI vêm a ser cada vez mais complexos.

Sendo assim, para que uma empresa possa tira total vantagem do uso de modernas estruturas de TI visando ganhar competitividade, e necessário que sejam tomadas algumas atitudes. E uma delas e a modernizando de seu parque computacional, pois a tecnologia da informação vem interferindo agressivamente em todas as áreas do negocio, bem como nos vários setores profissionais, sejam eles públicos ou privados. Direta ou indiretamente, todos fazem uso de algum serviço ou dispositivo sobre o qual a tecnologia de informação está sendo utilizada.

Todas as inspetorias e escritórios de representação estão equipados com computadores, impressoras e scanner, sendo os computadores destinados as atendentes, fiscais, sala dos profissionais e estagiários que usam equipamentos nas inspetorias.

Neste projeto, pretendemos imprimir maior segurança ao sistema de armazenamento de dados, aumentar a capacidade de armazenamento e a velocidade de recuperação dos dados, melhorar o sistema de proteção dos dados dos ataques externo, assim como aumentar a mobilidade e a qualidade de trabalho prestado pelos colaboradores do Conselho de forma a atender as metas estabelecidas no Plano Diretor de Tecnologia da Informação PDTI 2019-2020 e o projeto de estruturação tecnológica do ano 2019.

3. QUANTITATIVO E ESPECIFICAÇÕES TÉCNICAS DOS ITENS/OBJETOS.

3.1 A descrição dos materiais a serem adquiridas respectivas quantidades, consta indicado Abaixo:

ITEM	Descrição do Produto	Und.	Qt
01	Solução de Firewall Físico (Hardware) com serviços de Next Generation Firewall com **ADVANCED GATEWAY SECURITY SUITE** destinados à proteção da rede e controle do tráfego, contemplando o gerenciamento e monitoramento de todo o trafego do conselho; Performance de todos os serviços ativos de Threat Prevention, (Proteção Anti-Malware e Anti-virus, IDS, IPS e Controle de Aplicação) deverá ser de 1.5 Gbps ou superior. Caso o fornecedor não possa comprovar este item em documentações públicas, deve ser comprovado através de testes em bancada com gerador de pacotes (custos destes testes pagos pela CONTRATADA). Perfomance de Inspeção (decriptografia e criptografia) de trafego criptografado (SSL) de no mínimo 300 Mbps, os throughputs devem ser comprovados por documento de domínio público do fabricante. Caso o fornecedor não possa comprovar este item em documentações públicas, deve ser comprovado através de testes em bancada com gerador de pacotes (custos destes testes pagos pela CONTRATADA). Não serão aceitos declarações ou cartas de fabricantes para atendimento a este item; Performance de IPS de 1.4 Gbps ou superior Suporte a, no mínimo, 1.000.000 de conexões do tipo SPI simultâneas; Suporte a, no mínimo, 14.000 novas conexões por segundo; Disco interno SSD para amazenamento de no minimo 16 Gb Deve suportar fonte de alimentação interna redundante com chaveamento automático de 100-240 VAC. Deverá possuir pelo menos 4 interfaces de 2.5GbE SFP; Deverá possuir pelo menos 4 interfaces de 2.5GbE;	UND	01

	Deverá possuir pelo menos 12 interfaces de 1 GbE; 12 interfaces de rede 10/100/1000 base-TX. Todas as interfaces devem possuir mecanismo de autosense e seleção de modo half/full duplex. A seleção da velocidade e duplex deve ser realizada obrigatoriamente através da interface gráfica de gerenciamento. As interfaces devem suportar as seguintes atribuições: a) Segmento WAN , ou externo. b) Segmento WAN, secundário com possibilidade de ativação de recurso para redundância de WAN com balanceamento de carga e WAN Failover por aplicação. O equipamento deverá suportar no mínimo balanceamento de 4 links utilizando diferentes métricas pré-definidas pelo sistema e configuráveis pelo administrador. c) Segmento LAN ou rede interna. d) Segmento LAN ou rede interna podendo ser configurado como DMZ (Zona desmilitarizada) e) Segmento LAN ou rede interna ou Porta de sincronismo para funcionamento em alta disponibilidade f) Segmento ou Zona exclusiva para controle de dispositivos Wireless dedicado, com controle e configuração destes dispositivos. 01 (uma) interface do tipo console ou similar; 01 (uma) interface de rede dedicada para gerenciamento; A VPN Client-to-Site IPsec deve ser licenciada para, no mínimo, 50 usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para no mínimo, 1.000 usuários simultâneos, com aquisição de licença futura; A VPN SSL deve ser licenciada para, no mínimo, 2 usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para no mínimo, 350 usuários simultâneos, com aquisição de licença futura; Suportar 1.000 túneis de VPN IPSEC simultâneos; Suportar, no mínimo, 1.45 Gbps de throughput de VPN IPSEC Os Throughputs devem ser comprovados por documento de domínio público do fabricante. A ausência de tais documentos comprobatórios		

	reservará ao órgão o direito de aferir a performance dos equipamentos em bancada, assim como atendimento de todas as funcionalidades especificadas neste edital. Caso seja comprovado o não atendimento das especificações mínimas nos testes de bancada, o fornecedor será considerado inabilitados. Todos os custos oriundos do teste de bancada serão por conta do fornecedor; O fornecimento dos produtos e seus licenciamentos devem ser entregues através de empresa credenciada e autorizada pelo fabricante. Isto deve ser comprovada através de carta de reconhecimento assinada pelo representante legal do fabricante no Brasil. Não serão aceitas cartas ou declarações de fabricantes para atendimento aos valores de performance solicitados; "Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e/ou end-of-sale ou situação semelhante; CARACTERÍSTICAS GERAIS Todas as funcionalidades descritas devem funcionar no mesmo appliance sem a necessidade de composição de um ou mais produtos; A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7 O hardware e software que executem as funcionalidades de proteção de rede devem ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico; O equipamento deverá ser baseado em hardware desenvolvido com está finalidade, ou seja, não sendo aceita soluções baseadas em plataforma PC ou equivalente. Não serão permitidas soluções baseadas em sistemas operacionais abertos (OpenSource) como Free BSD, Debian ou mesmo Linux. Todo o ambiente deverá ser gerenciado através de uma única interface sem a necessidade de produtos de terceiros para compor a solução; Deve ser possível suportar arquitetura de armazenamento de logs redundante, permitindo a configuração de equipamentos distintos; A solução deverá suportar monitoramento através de SNMP v2 e v3;		

	Deve oferecer as funcionalidades de backup/restore tanto da configuração quanto do firmware/sistema operacional através da interface gráfica, assim como permitir ao administrador agendar procedimentos de backups da configuração em determinado dia e hora. O appliance deve armazenar no mínimo 02 (duas) versões distintas do sistema operacional, sendo possível escolher qual versão será inicalizada;de backups da configuração em determinado dia e hora. Suporte a definição de VLAN no firewall, conforme padrão IEEE 802.1q e ser possível criar sub-interfaces lógicas associadas a VLANs e estabelecer regras de filtragem (Stateful Firewall) entre elas; A solução deve suportar configuração de link-aggregation de interfaces suportando o protocolo 802.3ad para aumento de throughput . A solução deve suportar configuração de port-redundacy de interfaces para a alta disponibilidade de interfaces; Os dispositivos de proteção devem ter a capacidade de operar de forma simultânea mediante o uso de suas interfaces físicas nos seguintes modos: Modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3); Modo sniffer, para inspeção via porta espelhada do tráfego de dados da rede; Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação; 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; Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas. Possuir DHCP Server interno; Suporte a encaminhamento de pacotes UDPs multicast/broadcast entre diferentes interfaces e zonas de segurança como como DHCP Relay, suportando os protocolos e portas: Time service—UDP porta 37		

	DNS—UDP porta 53 DHCP—UDP portas 67 e 68 Net-Bios DNS—UDP porta 137 Net-Bios Datagram—UDP porta 138 Wake On LAN—UDP porta 7 e 9 mDNS—UDP porta 5353 Suporte a Jumbo Frames; Implementar sub-interfaces ethernet lógicas; Deve suportar os seguintes tipos de NAT: Nat dinâmico (Many-to-1); Nat dinâmico (Many-to-Many); Nat estático (1-to-1); NAT estático (Many-to-Many); Nat estático bidirecional 1-to-1; Tradução de porta (PAT); NAT de origem; NAT de destino; Suportar NAT de origem e NAT de destino simultaneamente. Prover mecanismo contra ataques de falsificação de endereços (IP Spoofing) Implementar mecanismo de sincronismo de horário através do protocolo NTP. Para tanto o appliance deve realizar a pesquisa em pelo menos 03 servidores NTP distintos, com a configuração do tempo do intervalo de pesquisa; Possuir gerenciamento de tráfego de entrada ou saida, por serviços, endereços IP e regra de firewall, permitindo definir banda mínima garantida e máxima permitida em porcentagem (%) para cada regra definida.		

	Implementar 802.1p e classe de serviços CoS (Class of Service) de DSCP (Differentiated Services Code Points); Permitir remarcação de pacotes utilizando TOS e/ou DSCP; Suporte a policy based routing (PBR), com a capacidade de roteamento por endereço de origem, endereço de destino, serviço, interface ou todas as opções simultâneas. Suportar protocolos de roteamento RIP, RIPng, OSPF, OSPFv3 e BGP; Suportar Equal Cost Multi-Path (ECMP) Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2); Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3, RIPng); A solução deve suportar integralmente o padrão IPv6, assim como criação de regras com objetos que utilizem endereços IPv4 e IPv6. Deve suportar no minimo as seguintes funcionalidades ou protocolos para o padrão de enderaçamento IPv6: Tunel 6 to 4, regras de acesso, objetos de enderço, limitador de conexões IPv6, monitor de conexões, DHCP, gerenciamento HTTPS via IPv6, NAT IPv6, proteção contra ataques to tipo IP Spoofing para IPv6, captura de pacotes IPv6, interface VLAN com endereço IPv6, VPN SSL com o uso do IPv6, controle de URL, Anti-Malware e anti-virus, controle de aplicação, IPS, IKEv2, ICMP6, SNMP, alta disponibilidade, RFC 1981 Path MTU Discovery for IPv6, RFC 2460 IPv6 specification, RFC 2464 Transmission of IPv6 Packets over Ethernet Networks; Possui suporte a log via syslog; Possuir mecanismo para possibilitar a aplicação de correções e atualizações para o firewall remotamente através da interface gráfica; Permitir a visualização em tempo real de todas as conexões TCP e sessões UDP que se encontrem ativas através do firewall. Permitir a geração de gráficos em tempo real, representando os serviços mais utilizados e as máquinas mais acessadas em um dado momento; Permitir a visualização de estatísticas do uso de CPU do appliance o		

	através da interface gráfica remota em tempo real; A solução deverá suportar a tecnologia de SD-WAN e deverá ter no mínimo as seguintes funcionalidades: Capacidade de criar um overlay virtual de roteamento, de forma agnóstica a infraestrutura de rede já existente, com a combinação de quaisquer tipos de circuitos WAN; Capacidade de agregar no mínimo 3 (três) circuitos WAN distintos em um único canal lógico; Implementar segurança fim-a-fim usando solução de criptografia que de maneira automática forneça proteção à redes WANs privadas que transitam por redes públicas compartilhadas; Suportar e implementar QoS com classificação, marcação e priorização de tráfego com base em endereço IP de origem/destino, portas TCP/UDP de origem e destino, DSCP (Differentiated Services Code Point), tipo de aplicação camada 7 e traffic shaping nas interfaces; Capacidade de realizar a saída local de internet para alguns tráfegos selecionados a partir, no mínimo, dos parâmetros de IP, porta e URL; Controle de caminho automático baseado em políticas, com habilidade de selecionar o caminho, no mínimo, através dos seguintes parâmetros simultâneos ou não: a. tipo de aplicação; b. prioridade de negócio; c. latência; d. jitter; e. perda de pacotes. d) A comutação dos caminhos deve ocorrer de maneira dinâmica e automática baseada nas políticas previamente aplicadas. e) Permitir a alteração da política de encaminhamento sem impacto no tráfego. f) Implementar tecnologia de reconhecimento de aplicações conhecidas (DPI), como Office 365, Facebook e Youtube, como também subaplicações associadas como Facebook Messenger e Office 365		

	Outlook. Alta Disponibilidade A solução deve ter disponibilidade para operar em alta disponibilidade no modo Ativo/Standby, com as implementações de Failover. Não serão permitidas soluções de cluster (HA) que façam com que o equipamento (s) reinicie após qualquer modificação de parâmetro/configuração seja realizada pelo administrador. A solução deve ter capacidade de fazer monitoramento físico das interfaces dos membros do cluster. A solução deve ter disponibilidade para operar em alta disponibilidade implementando monitoramento logico de um host na rede, para verificar a existência de problemas lógicos na rede e possibilitar failover. A solução deve permitir o uso de endereço MAC virtual para evitar problemas de expiração de tabela ARP em caso de Failover. A solução deve possibilitar a sincronização de todas as configurações realizadas na caixa principal do cluster, incluído, mas não limitado a objetos, regras, rotas, VPNs e politicas de segurança. A solução deve permitir visualizar no equipamento principal, o status da comunicação entre o peers do cluster, status de sincronização das configurações, status atual equipamento backup. VPN Criptografia 3DES, AES 128 e AES 256; Autenticação com MD5, SHA-1, SHA-256 e SHA-384; Diffie-Hellman: Grupo 2 (1024 bits), Grupo 5 (1536 bits) e Grupo 14 (2048 bits; Algoritmo Internet Key Exchange (IKE);		

	Autenticação via certificado IKE PKI; Deve possuir interoperabilidade com outros fabricantes de acordo com o padrão IPSEC através de RFC`s; A solução deve suportar VPNs L2TP, incluindo suporte para iPhone, Windows phone, Android com suporte a cliente L2TP; Solução deve suportar VPNs baseadas em politicas e VPNs baseadas em roteamento estatico e dinâmico. Suportar políticas de roteamento sobre conexões VPN IPSEC do tipo site-to-site com diferentes métricas e serviços. A rota poderá prover aos usuários diferentes caminhos redundantes sobre todas as conexões VPN IPSEC. Solução deve incluir a capacidade de estabelecer VPNs com outros firewalls que utilizam IP públicos dinâmicos; Permitir a definição de um gateway redundante para terminação de VPN no caso de queda do circuito primário; Permitir que seja criado politicas de roteamentos estáticos utilizando IPs de origem, destino, serviços e a própria VPN como parte encaminhadora deste tráfego sendo este visto pela regra de roteamento, como uma interface simples de rede para encaminhamento do tráfego. Suportar a criação de túneis IP sobre IP (IPSEC Tunnel), de modo a possibilitar que duas redes com endereço inválido possam se comunicar através da Internet; Autenticação Permitir a utilização de LDAP, AD e RADIUS; Permitir o cadastro manual dos usuários e grupos diretamente na interface de gerencia remota do Firewall, caso onde se dispensa um autenticador remoto para o mesmo; Suporte a uma rede com multiplus domínios, possibilitando a integração em um ambiente onde existas domínios diferentes e totalmente segregados.		

	Permitir a integração com qualquer autoridade certificadora emissora de certificados X509 que seguir o padrão de PKI descrito na RFC 2459, inclusive verificando as CRLs emitidas periodicamente pelas autoridades, que devem ser obtidas automaticamente pelo firewall via protocolos HTTP e LDAP; Permitir o controle de acesso por usuário, para plataformas Windows Me, NT, 2000, 2000, XP, Windows 7 , Windows 8 e Windows 10 de forma transparente, para todos os serviços suportados, de forma que ao efetuar o logon na rede, um determinado usuário tenha seu perfil de acesso automaticamente configurado; Permitir a restrição de atribuição de perfil de acesso a usuário ou grupo independente ao endereço IP da máquina que o usuário esteja utilizando. Suportar recurso de autenticação única para todo o ambiente de rede, ou seja, utilizando a plataforma de autenticação atual que pode ser de LDAP ou AD; o perfil de cada usuário deverá ser obtido automaticamente através de regras no Firewall DPI (Deep Packet Inspection) sem a necessidade de uma nova autenticação como por exemplo, para os serviços de navegação a Internet atuando assim de forma toda transparente ao usuário. Serviços como HTTP, HTTPS devem apenas consultar uma base de dados de usuários e grupos de servidores 2008/2012 com AD; IPS Para proteção de ambientes contra-ataques, os dispositivos de proteção devem possuir módulo de IPS integrados no próprio appliance de firewall, onde sua console de gerência deverá residir na mesma console centralizada dos appliances de segurança, com suporte a pelo menos 3.000 assinaturas; A solução de IPS deverá possuir os seguintes mecanismos de detecção: assinaturas e trabalhar em conjunto com o controle de aplicações; A solução de IPS deve fazer a inspeção de todo o pacote, independentemente do tamanho; A solução de IPS deve fazer a inspeção de todo o trafego de forma bidirecional, analisando qualquer tamanho de pacote sem degradar a		

	performance do equipamento solicitada neste edital; Possuir capacidade de remontagem de pacotes para identificação de ataques; O mecanismo de inspeção deve receber e implementar em tempo real atualizações para os ataques emergentes sem a necessidade de reiniciar o appliance; Para cada proteção de segurança, deve ser possível consultar informações no site do fabricante. A ferramenta de log deve possuir a capacidade de criar uma regra de exceção a partir do log visualizado na gerência centralizada; As regras de exceção devem possuir: origem, destino e serviço; A solução deve ser capaz de inspecionar tráfego HTTPS. Deverá possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep; Detecção de anomalias; A solução de IPS deve possuir política capaz de definir o modo de operação (bloqueio ou detecção); O módulo de IPS deve possuir assinaturas voltadas para ambientes de servidores de SMTP, Web e DNS; O mecanismo de inspeção deve receber e implementar em tempo real atualizações de novas assinaturas sem a necessidade de reiniciar o appliance; Para cada proteção, ou para todas as proteções suportadas, deve incluir a opção de adicionar exceções baseado na origem e destino; A solução deve ser capaz de detectar e bloquear ataques nas camadas de rede e aplicação, protegendo pelo menos os seguintes serviços: Aplicações web, serviços de e-mail, DNS, FTP, SQL Injection, ataques a sistemas operacionais e VOIP; Deve incluir proteção contra worms; Deve incluir uma tela de visualização situacional a fim de monitorar graficamente a quantidade de alertas de diferentes severidades e a		

	evolução ao logo do tempo dispondo o sumario quantitativo das ameaças analisadas. A solução deve possuir esquema de atualização de assinaturas através de um click; Atualização de modo offline, onde poder ser baixado na base do fabricante e posteriormente fazer o upload do arquivo na solução; A solução deve suportar importar certificados de servidor para inspeções de tráfego seguro HTTP (HTTPS) de entrada. Depois de importar esses certificados, a solução deve permitir o IPS para Inspeção segura HTTP(HTTPS); A solução deverá ser capaz de inspecionar e proteger apenas hosts internos; A solução deverá possuir proteções para sistemas SCADA; Solução deverá permitir que o administrador bloqueie facilmente o tráfego de entrada e/ou saída com base em países, sem a necessidade de gerir manualmente os ranges de endereços IP dos países que deseja bloquear. Aplication Control Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades abaixo: Deve ser possível a liberação e bloqueio de aplicações sem a necessidade de liberação de portas e protocolos. Capacidade para realizar filtragens/inspeções dentro de portas TCP conhecidas, por exemplo, porta 80 http, buscando por aplicações que potencialmente expõe o ambiente como: P2P, Kazaa, Morpheus, BitTorrent ou messengers Controlar o uso dos serviços de Instant Messengers como MSN, YAHOO, Google Talk, ICQ, de acordo com o perfil de cada usuário ou grupo de usuários, de modo a definir, para cada perfil, se ele pode ou não realizar download e/ou upload de arquivos, limitar as extensões dos arquivos que		

	podem ser enviados/recebidos e permissões e bloqueio de sua utilização baseados em horários pré-determinados pelo administrador será obrigatório para este item. Deverá controlar software FreeProxy tais como ToR, Ultrasurf, Freegate,etc. Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem; Deverá permitir a criação de regras para acesso/bloqueio por subrede de origem e destino; Atualizar a base de assinaturas de aplicações automaticamente; Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos do LDAP/AD; A solução de controle de aplicação WEB deve criar regras granulares possibilitando adicionar tipos de aplicação WEB e categorias por regra, sendo assim criando controle granular de qualquer tipo de acesso não permitido pela empresa; Deve implementar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e protocolos; Caso a solução não tenha assinaturas pré-definida na solução a mesma deverá possibilitar a criação ou importação de assinaturas personalizadas para os seguintes tipos ou protocolos: HTTP, FTP, Email e extensão de arquivos. O administrador deve ser capaz de configurar quais comandos FTP são aceitos e quais são bloqueados a partir de comandos FTP pré-definidos; Deve possibilitar que o controle de portas seja aplicado para todas as aplicações; Deverá possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, uTorrent, etc.) possuindo granularidade de controle/políticas para os mesmos; Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Facebook e bloquear chat; Deverá possibilitar a diferenciação de aplicações Proxies possuindo		

	granularidade de controle/políticas para os mesmos; Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como: Nível de risco da aplicação. Categoria de aplicações. Filtro de URL Para prover maior visibilidade e controle dos acessos dos usuários do ambiente, deve ser incluído um módulo de filtro de URL integrado no firewall; Possuir base contendo no mínimo 20 milhões de sites internet web já registrados e classificados com atualização automática; Implementar filtro de conteúdo transparente para o protocolo HTTP, de forma a dispensar a configuração dos browsers das máquinas clientes. A plataforma de proteção deve possuir as seguintes funcionalidades de filtro de URL: Permitir a criação de listas personalizadas de URLs permitidas e bloqueadas (lista branca e lista negra); Permitir especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora); Deve ser possível à criação de políticas por usuários, grupos de usuários, IPs, redes e grupos de redes; O mecanismo de Controle de aplicação Web/URL deve apresentar contagem de utilização de regra de acordo com a utilização (hit count); Deverá permitir criar política de confirmação de acesso Deve possibilitar a inspeção de tráfego HTTPS (Inbound/Outbound), sendo que para a opção de Outbound não será necessário efetuar o "man-inthe- middle", ou seja, a solução deverá prover mecanismo que irá		

	analisar a conexão HTTPS para verificar se a URL solicitada está na lista de permissões de acesso, de acordo com a política configurada; O administrador poderá adicionar filtros por palavra-chave de modo específico; Deverá permitir o bloqueio Web através de senha pré configura pelo administrador Deverá 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); A solução deve fornecer um mecanismo para solicitação de categorização de URL caso esta não esteja categorizada ou categorizada incorretamente; Suportar recurso de autenticação única para todo o ambiente de rede, ou seja, utilizando a plataforma de autenticação atual que pode ser de LDAP ou AD; o perfil de cada usuário deverá ser obtido automaticamente para o controle das políticas de Filtro de Conteúdo sem a necessidade de uma nova autenticação. Suportar a criação de políticas baseadas no controle por URL e categoria de URL; Suportar base ou cache de URLs local no appliance ou possibilitar a replicação da base de conhecimento de URLs do fabricante via instalação de maquina virtual, a infraestrutura da maquina virtual (VM) para uso desse recurso será fornecida pelo CONTRATANTE , evitando delay de comunicação/validação das URLs; Possuir pelo menos 50 categorias de URLs; Suporta a criação de categorias de URLs customizadas; Suporta a exclusão de URLs do bloqueio, por categoria; Deverá possibilitar a categorização ou recategorização de URL caso não esteja categorizada ou categorizada incorretamente; A solução deverá permitir um mecanismo que permita sobrescrever as		

	categorias de URL; Permite a customização de página de bloqueio; PROTEÇÃO CONTRA VIRUS E BOT-NETS Deve possuir módulo de antivírus e anti-bot integrado no próprio appliance de segurança ; A solução de anti-virus integrada deve ter capacidade de analisar arquivos maiores que 1Gbps. A solução deve possuir nuvem de inteligência proprietária do fabricante onde seja responsável em atualizar toda a base de segurança dos appliances através de assinaturas. Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e qualquer outro mecanismo de redirecionamento de tráfego; Implementar funcionalidade de detecção e bloqueio de callbacks; A solução deverá ser capaz de detectar e bloquear comportamento suspeito ou anormal da rede; A solução Antibot deve possuir mecanismo de detecção que inclui, reputação de endereço IP; Implementar interface gráfica WEB segura, utilizando o protocolo HTTPS. Implementar interface CLI segura através do protocolo SSH; Possuir antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, IMAP, POP3, FTP, CIFS e TCP Stream; A solução deve permitir criar regras de exceção de acordo com a proteção; Deve possuir visualização na própria interface de gerenciamento referente aos top incidentes através de hosts ou incidentes referentes a		

	incidentes de vírus e Bots; Permitir o bloqueio de malwares (vírus, worms, spyware e etc) A solução deve ser capaz de proteger contra ataques para DNS. A solução deverá ser gerenciada a partir de uma console centralizada com políticas granulares A solução deve ser capaz de prevenir acesso a websites maliciosos. A solução deve ser capaz de realizar inspeção de tráfego SSL e SSH. A solução deverá receber atualizações de um serviço baseado em cloud. A solução deverá ser capaz de bloquear a entrada de arquivos maliciosos. A solução Antivírus deverá suportar análise de arquivos que trafegam dentro do protocolo CIFS. A solução deve suportar funcionalidade de GeoIP, ou seja, a capacidade de identificar, isolar e controlar tráfego baseado na localização (origem e/ou destino), incluindo a capacidade de configuração de listas customizadas para esta mesma finalidade. PROTEÇÃO CONTRA ATAQUES AVANÇADOS A solução deverá prover as funcionalidades de inspeção de tráfego de entrada e saída de malwares não conhecidos ou do tipo APT com filtro de ameaças avançadas e análise de execução em tempo real, e inspeção de tráfego de saída de callbacks; Suportar os protocolos HTTP assim como inspeção de tráfego criptografado através de HTTPS e TLS; A solução deve ser capaz de inspecionar o tráfego criptografado SSL e SSH; Identificar e bloquear a existência de malware em comunicações de entrada e saída, incluindo destinos de servidores do tipo Comando e Controle; Implementar mecanismo de bloqueio de vazamento não intencional de		

	dados oriundos de máquinas existentes no ambiente LAN em tempo real; Implementar detecção e bloqueio imediato de malwares que utilizem mecanismo de exploração em arquivos no formato PDF, sendo que a solução deve inspecionar arquivo PDF com até 10Mb; Implementar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows e Android; Conter ameaças de dia zero permitindo ao usuário final o recebimento do arquivos livres de malware; A tecnologia de máquina virtual deverá suportar diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso sem utilização de assinaturas; A solução deve possuir nuvem de inteligência proprietária do fabricante onde seja responsável em atualizar toda a base de segurança dos appliance através de assinaturas. Implementar a visualização dos resultados das análises de malwares de dia zero nos diferentes sistemas operacionais dos ambientes controlados (sandbox) suportados; Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e qualquer outro mecanismo de redirecionamento de tráfego; Conter ameaças avançadas de dia zero; Toda análise deverá ser realizada de forma automatizada sem a necessidade de criação de regras específicas e/ou interação de um operador; Implementar mecanismo do tipo múltiplas fases para verificação de malware e/ou códigos maliciosos; Toda a análise e bloqueio de malwares e/ou códigos maliciosos deve ocorrer em tempo real. Não serão aceitas soluções que apenas detectam o malware e/ou códigos maliciosos; Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx) e Android APKs no ambiente controlado; Implementar a análise de arquivos executáveis, DLLs, ZIP e criptografados		

	em SSL no ambiente controlado; Possuir antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, POP3, FTP , IMAP e CIFS; Conter ameaças de dia zero de forma transparente para o usuário final; Conter ameaças de dia zero através de tecnologias em nível de emulação e código de registro; Implementar mecanismo de pesquisa por diferentes intervalos de tempo; Conter ameaças de dia zero via tráfego de internet; Permitir a contenção de ameaças de dia zero sem a alteração da infraestrutura de segurança; Conter ameaças de dia zero que possam burlar o sistema operacional emulado; A solução deve permitir a criação de White list baseado no MD5 do arquivo; Conter ameaças de dia zero antes da execução e evasão de qualquer código malicioso; Conter exploits avançados. A análise “In Cloud” ou local deve prover informações sobre as ações do Malware na máquina infectada, informações sobre quais aplicações são utilizadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo Malware, gerar assinaturas de Antivírus e Antispyware automaticamente, definir URLs não confiáveis utilizadas pelo novo Malware e prover Informações sobre o usuário infectado (seu endereço IP e seu login de rede); Suporte a submissão manual de arquivos para análise através do serviço de Sandbox ADMINISTRAÇÃO Suportar no mínimo 20.000 usuários autenticados com serviços ativos e		

	identificados passando por este dispositivo de segurança em um único dispositivo de segurança. Políticas baseadas por grupos de usuários deverão ser suportadas por este dispositivo. Está comprovação poderá ser exigida em testes sobe o ambiente de produção com o fornecimento do produto para comprovação deste e demais itens. Permitir a criação de perfis de administração distintos, de forma a possibilitar a definição de diversos administradores para o firewall, cada um responsável por determinadas tarefas da administração; Fornecer gerência remota, com interface gráfica nativa; A interface gráfica deverá possuir assistentes para facilitar a configuração inicial e a realização das tarefas mais comuns na administração do firewall, incluindo a configuração de VPN IPSECs, NAT, perfis de acesso e regras de filtragem; Possuir mecanismo que permita a realização de cópias de segurança (backups) e sua posterior restauração remotamente, através da interface gráfica, sem necessidade de se reinicializar o sistema; Possuir mecanismo para possibilitar a aplicação de correções e atualizações para o firewall remotamente através da interface gráfica; Permitir a visualização em tempo real de todas as conexões TCP e sessões UDP que se encontrem ativas através do firewall e a remoção de qualquer uma destas sessões ou conexões; Permitir a geração de gráficos em tempo real, representando os serviços mais utilizados e as máquinas mais acessadas em um dado momento; Permitir a visualização de estatísticas do uso de CPU, memória da máquina onde o firewall está rodando e tráfego de rede em todas as interfaces do Firewall através da interface gráfica remota, em tempo real e em forma tabular e gráfica; Permitir a conexão simultânea de vários administradores, sendo um deles com poderes de alteração de configurações e os demais apenas de visualização das mesmas. Permitir que o segundo ao se conectar possa enviar uma mensagem ao primeiro através da interface de administração. Possibilitar o registro de toda a comunicação realizada através do firewall, e de todas as tentativas de abertura de sessões ou conexões que		

	forem recusadas pelo mesmo; Possuir interface orientada a linha de comando para a administração do firewall a partir do console ou conexão SSH sendo está múltiplas sessões simultâneas. Possuir mecanismo que permita inspecionar o tráfego de rede em tempo real (sniffer) via interface gráfica, podendo opcionalmente exportar os dados visualizados para arquivo formato PCAP e permitindo a filtragem dos pacotes por protocolo, endereço IP origem e/ou destino e porta IP origem e/ou destino, usando uma linguagem textual; Permitir a visualização do tráfego de rede em tempo real tanto nas interfaces de rede do Firewall quando nos pontos internos do mesmo: anterior e posterior à filtragem de pacotes, onde o efeito do NAT (tradução de endereços) é eliminado; Possuir sistema de respostas automáticas que possibilite alertar imediatamente o administrador através de e-mails, janelas de alerta na interface gráfica, execução de programas e envio de Traps SNMP; Relatórios Ser capaz de visualizar, de forma direta no appliance e em tempo real, as aplicações mais utilizadas, os usuários que mais estão utilizando estes recursos informando sua sessão, total de pacotes enviados, total de bytes enviados e média de utilização em Kbps, URLs acessadas e ameaças identificadas. Possibilitar a geração de pelo menos os seguintes tipos de relatório com cruzamento de informações, mostrados em formato HTML: máquinas acessadas X serviços bloqueados, usuários X URLs acessadas, usuários X categorias Web bloqueadas (em caso de utilização de um filtro de conteúdo Web); Possibilitar a geração de pelo menos os seguintes tipos de relatório, mostrados em formato HTML: máquinas mais acessadas, serviços mais utilizados, usuários que mais utilizaram serviços, URLs mais visualizadas, ou categorias Web mais acessadas (em caso de existência de um filtro de conteúdo Web), maiores emissores e receptores de e-mail; Permitir o envio dos relatórios, através de email para usuários		

	prédefinidos; Possuir relatórios pré-definidos na solução e permitir a criação de relatórios customizados; Possibilitar a geração dos relatórios sob demanda e através de agendamento diário, semanal e mensal. No caso de agendamento, os relatórios deverão ser publicados de forma automática Disponibilizar download dos relatórios gerados; Deverá ser entregue solução composto de appliance ou máquina virtual únicos ou composição de appliances ou maquinas virtuais, de forma a atender a todos os requisitos solicitados sem perda de funcionalidade. Em caso de appliance o hardware deve ser do mesmo fabricante do equipamento de firewall Caso a solução entregue utilize virtualização deverá ser compatível com VMware vSphere 5 ou superior; Caso seja fornecida em appliance, ao mínimo 16 GB de memória RAM Caso a solução seja fornecida em appliance, o armazenamento total em disco deverá ser de no mínimo 1TB. Estes discos poderão ainda ser substituídos pela contratante / contratada sem a paralisação parcial ou total do sistema. Fornecer gerência remota, com interface gráfica nativa, através do aplicativo ActiveX ou Java. Fornecer interface gráfica para no mínimo 5 usuários; A interface gráfica deverá possuir mecanismo que permita a gerência e emissão de relatórios de forma remota Possibilitar a geração de pelo menos os seguintes tipos de relatório, mostrados em formato HTML, PDF e CSV: máquinas mais acessadas, serviços mais utilizados, usuários que mais utilizaram serviços, URLs mais visualizadas, ou categorias Web mais acessadas (em caso de existência de um filtro de conteúdo Web), maiores emissores e receptores de e-mail, detecção de intrusos, intrusos bloqueados e alvos, para vírus e spywares bloqueados, alvos e detectados. Possibilitar a geração de pelo menos os seguintes tipos de relatório com cruzamento de informações, mostrados em formato HTML: máquinas acessadas X serviços bloqueados, usuários X URLs acessadas, usuários X		

	categorias Web bloqueadas (em caso de utilização de um filtro de conteúdo Web); Possibilitar a geração de pelo menos os seguintes tipos de relatório com cruzamento de informações, mostrados em formato HTML: máquinas acessadas X serviços bloqueados, usuários X URLs acessadas, usuários X categorias Web bloqueadas (em caso de utilização de um filtro de conteúdo Web); Prover mecanismo de visualização de eventos em tempo real das funções de segurança, com uma prévia sumarização para fácil visualização de no mínimo as seguintes informações: Aplicações mais utilizadas; Usuários com maior atividade; Estatísticas de uso; Principais aplicações por taxa de transferência de bytes; Principais hosts por número de ameaças identificadas; Prover mecanismo de consulta às informações registradas integrado à interface de administração; Possibilitar o armazenamento de seus registros (log e/ou eventos) Possibilitar a recuperação dos registros de log e/ou eventos armazenados em máquina remota, através de protocolo criptografado, de forma transparente através da interface gráfica; Possibilitar a análise dos seus registros (log e/ou eventos) por pelo menos um programa analisador de log disponível no mercado; Prover mecanismo de visualização de eventos em tempo real das funções de segurança, com uma prévia sumarização para fácil visualização de no mínimo as seguintes informações: Aplicações mais utilizadas; Usuários com maior atividade; Estatísticas de uso; Principais aplicações por taxa de transferência de bytes;		

	Principais hosts por número de ameaças identificadas; Garantia, Suporte e Licenciamento O licenciamento para todos os serviços de Next Generation Firewall (**ADVANCED GATEWAY SECURITY SUITE**) deverá ser de 60 meses. A garantia deverá ser de 60 meses e compor juntamente a garantia do hardware (equipamento físico). Deve contemplar suporte do Fabricante pelo período vigente. Com no mínimo, as seguintes características: a. O suporte do fabricante deve ter um sistema de abertura de chamados para acompanhamento – funcionando 24 horas por dia e 7 dias por semana. Para atendimento telefônico, deve operar em língua Portuguesa pelo menos em regime 8x5. b. Deve assegurar a utilização de novas versões de software da solução sem ônus a Licitante, sempre que esta estiver disponível a qualquer cliente. c. Deve permitir o acesso à base de conhecimento da solução. Conformidade a) O Fabricante deve comprovar participação no MAPP da Microsoft; b) A tecnologia deve possuir pelo menos uma certificação da ICSA Labs, ICSA Firewall ou Antivirus; c) O fabricante da solução deverá ser avaliado pela NSS Labs (Network Security Services) no desempenho do Next Generation Firewall Comparative Analysis mais recente, estando no “Security Value Map” acima de 90 % (noventa por cento) da avaliação de segurança efetiva. d) No momento da entrega dos equipamentos a proponente vencedora deverá fornecer declaração do(s) fabricante(s), em papel timbrado com firma reconhecida, dos produtos ofertados, declarando que a		

	proponente possui credenciamento do mesmo para a implantação e suporte técnico de seus produtos; e) Deve ser homologado pela ANATEL. - O equipamento deve ser do tipo 1U Rack; -Deve ser acompanhado de todos os acessórios necessários para operacionalização do equipamento, tais como: softwares, licenças, documentação técnica e manual. - Se o item proposto nesse termo for descontinuado tanto no ato quanto após a homologação do processo deverá ser informado para possível aceite de outro produto de qualidade equivalente ou superior pelo mesmo preço.		

3.2 Cabem à empresa fornecedora avisar por escrito, após verificação das especificações discriminativas, todos os erros, incoerências ou divergências que possam ser levantadas através destas especificações, para que se tomem as devidas providências, não aceitando, posteriormente, qualquer alegação de desconhecimento, incompreensão, dúvidas ou esquecimento de qualquer detalhe**.**

4 DO CUSTO ESTIMADO.

De acordo com o § 2º do art. 9º do Decreto nº 5450/2005, os valores estimados da presente aquisição do (s) referido objeto (s) será verificado através da pesquisa de mercado.

5. DA DOTAÇÃO ORÇAMENTARIA.

As despesas advindas do presente processo ocorrerão no exercício de 2019/2020, orçamento Prodesu à conta da rubrica 6.2.2.1.1.02.01.03.0.07 – Sistemas de Processamento de Dados.

6. DAS OBRIGAÇÕES DA CONTRATADA.

6.1. A Contratada deve cumprir todas as obrigações constantes no Edital, seus anexos e sua proposta, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto e, ainda:

6.1.1. Efetuar a entrega do objeto em perfeitas condições, conforme especificações, prazo e local constantes no Edital e seus anexos, acompanhado da respectiva nota fiscal, na qual constarão as indicações referentes á:

6.1.2. Responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com os artigos 12, 13 e17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990);

6.1.3. Substituir, reparar ou corrigir, às suas expensas, no prazo fixado neste Termo de Referência, o objeto com avarias ou defeitos;
6.1.4. Comunicar à Contratante, no prazo máximo de 24 (vinte e quatro) horas que antecede a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação;
6.1.5. Manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;
6.1.6. Indicar preposto para representá-la durante a execução do contrato.

7. DAS OBRIGAÇÕES DA CONTRATANTE.

7.1. São obrigações da Contratante:
7.1.1. Receber o objeto no prazo e condições estabelecidas no Edital e seus anexos;
7.1.2. Verificar minuciosamente, no prazo fixado, a conformidade dos bens recebidos provisoriamente com as especificações constantes do Edital e da proposta, para fins de aceitação e recebimento definitivo;
7.1.3. Comunicar à Contratada, por escrito, sobre imperfeições, falhas ou irregularidades verificadas no objeto fornecido, para que seja substituído, reparado ou corrigido;
7.1.4. Acompanhar e fiscalizar o cumprimento das obrigações da Contratada, através de comissão/servidor especialmente designado;
7.1.5. Efetuar o pagamento à Contratada no valor correspondente ao fornecimento do objeto, no prazo e forma estabelecidos no Edital e seus anexos;
7.2. A Administração não responderá por quaisquer compromissos assumidos pela Contratada com terceiros, ainda que vinculados à execução do presente Termo de Contrato, bem como por qualquer dano causado a terceiros em decorrência de ato da Contratada, de seus empregados, prepostos ou subordinados.

8. DAS CONDIÇÕES E RECEBIMENTO DO OBJETO.

8.1. A entrega dos materiais deverá ser atestada pelo Órgão Contratante, que aferirá a sua conformidade com as especificações constantes neste Termo de Referência.
8.2. O servidor designado para acompanhar a entrega do objeto formalizará o seu recebimento na própria nota fiscal e/ou fatura correspondente, no prazo máximo de 05(cinco) dias úteis contados da data da entrega do objeto, pela Contratada.
8.3. A Contratada se obriga a efetuar, a qualquer tempo, a substituição de material rejeitado, se este apresentar defeito de fabricação ou divergências relativas às especificações, independentemente da quantidade rejeitada.

9. GARANTIA

9.1 Os materiais deverão ter prazo de validade de, no mínimo 12(doze) meses, contados a partir da data da entrega sendo a garantia/licenciamento de 60 Meses.

10. CONTROLE DA EXECUÇÃO

10.1. Nos termos do art. 67 Lei nº 8.666, de 1993, será designado representante para acompanhar e fiscalizar a entrega dos bens, anotando em registro próprio todas as ocorrências relacionadas com a execução e determinando o que for necessário à regularização de falhas ou defeitos observados.

10.1.1. O recebimento de material de valor superior a R$ 80.000,00 (oitenta mil reais) será confiado a uma comissão de, no mínimo, 3 (três) membros, designados pela autoridade competente.

10.2. A fiscalização de que trata este item não exclui nem reduz a responsabilidade da Contratada, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas ou vícios redibitórios, e, na ocorrência desta, não implica em corresponsabilidade da Administração ou de seus agentes e prepostos, de conformidade com o art. 70 da Lei nº 8.666, de 1993.

10.3. O representante da Administração anotará em registro próprio todas as ocorrências relacionadas com a execução do contrato, indicando dia, mês e ano, bem como o nome dos funcionários eventualmente envolvidos, determinando o que for necessário à regularização das falhas ou defeitos observados e encaminhando os apontamentos à autoridade competente para as providências cabíveis.

11. ENTREGA E CRITÉRIOS DE ACEITAÇÃO DO OBJETO.

11.1 O prazo de entrega dos bens é de 30 (trinta) dias, contados em remessa Única, no seguinte endereço:

Conselho Regional de Engenharia e Agronomia de Rondônia.
Rua Elias Gorayeb, 2596 - bairro Liberdade. CEP: 76803-903 - Porto Velho-RO.
Seção de Almoxarifado do Departamento Administrativo.
Fone: (69) 2181-1061
Horário de recebimento: das 08h:00min às 14h:00min horário local de segunda a sexta-feira.

11.2. Os materiais serão recebidos provisoriamente no prazo de 5 dias, pelo (a) responsável pelo acompanhamento e fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes neste Termo de Referência e na proposta.

11.3. Os Materiais poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser substituídos no prazo de 02 dias, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades.

11.4. Os materiais serão recebidos definitivamente no prazo de 10 dias, contados do recebimento provisório, após a verificação da qualidade e quantidade do material e consequente aceitação mediante termo circunstanciado.

11.4.1. Na hipótese de a verificação a que se refere o subitem anterior não ser procedida dentro do prazo fixado, reputar-se-á como realizada, consumando-se o recebimento definitivo no dia do esgotamento do prazo.

11.5. O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da contratada pelos prejuízos resultantes da incorreta execução do contrato.

12. DA ACEITAÇÃO E DO PAGAMENTO.

12.1. Os materiais objeto deste Termo de Referência deverão ser analisados e aceitos pelo fiscal do contrato até o 5º dia útil após a apresentação da nota fiscal/fatura. Devidamente acompanhada de toda a documentação legal, datas nas quais encaminhará o faturamento à Gerência Financeira.
12.2. O pagamento será efetuado através de Ordem Bancária, até o 10º (décimo) dia útil após entrega da Nota Fiscal atestada pelo servidor designado.
a) Entregue a Contratante a nota fiscal/ fatura devidamente preenchida;
b) Indique o banco, a agência e a conta bancária da empresa, onde deverão ser depositados os valores referentes aos serviços prestados;
c) Entregue prova de regularidade, disponibilizando para consulta, via web, com o Instituto Nacional do Seguro Social (INSS), mediante apresentação da Certidão Negativa de Débitos (CND) Federal, Estadual e Municipal, com o Fundo de Garantia do Tempo de Serviço (FGTS), através do Certificado de Regularidade do FGTS (CRF), emitido pela Caixa Econômica Federal e CNDT.
d) Se optante do SIMPLES, entregue o Termo de Opção, conforme legislação.
e) Serão processadas as retenções previdenciárias e tributárias nos termos da lei que regula a matéria, conforme o caso.

13. DAS PENALIDADES.

13.1. Em caso de inexecução parcial ou total das condições pactuadas, erro ou mora na execução, garantida a prévia defesa, ficará a futura CONTRATADA sujeita às sanções previstas na Lei 8.666/93, sem prejuízo das responsabilidades civil e criminal que seu ato ensejar e Legislação pertinente.

14. DAS SANÇÕES ADMINISTRATIVAS.

14.1. Comete infração administrativa nos termos da Lei nº 8.666, de 1993 a Contratada que:
14.1.1 Executar total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação;
14.1.2 Ensejar o retardamento da execução do objeto;
14.1.3 Fraudar na execução do contrato;
14.1.4 Comportar-se de modo inidôneo;
14.1.5 Cometer fraude fiscal;
1.1.6 Não mantiver a proposta.
14.2 A Contratada que cometer qualquer das infrações discriminadas no subitem acima ficará sujeita, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:
14.2.1 advertência por faltas leves, assim entendidas aquelas que não acarretem prejuízos significativos para a Contratante;
14.2.2 Multa moratória de 5% (cinco por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 1 (um) dia;
14.2.3 multa compensatória de 5% (por cento) sobre o valor total do contrato, no caso de inexecução total do objeto;
14.2.4 em caso de inexecução parcial, a multa compensatória, no mesmo percentual do subitem acima, será aplicada de forma proporcional à obrigação inadimplida;
14.2.5 suspensão de licitar e impedimento de contratar com o órgão, entidade ou unidade administrativa pela qual a Administração Pública opera e atua concretamente, pelo prazo de até dois anos;
14.2.6 impedimento de licitar e contratar com a União com o consequente descredenciamento no SICAF pelo prazo de até cinco anos;
14.2.7 declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante

a própria autoridade que aplicou a penalidade, que será concedida sempre que a Contratada ressarcir a Contratante pelos prejuízos causados;

14.3 Também ficam sujeitas às penalidades do art. 87, III e IV da Lei nº 8.666, de 1993, a Contratada que:

14.3.1 tenha sofrido condenação definitiva por praticar, por meio dolosos, fraude fiscal no recolhimento de quaisquer tributos;

14.3.2 tenha praticado atos ilícitos visando a frustrar os objetivos da licitação;

14.3.3 demonstre não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.

14.4 A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à Contratada, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente a Lei nº 9.784, de 1999.

14.5 A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

14.6 As penalidades serão obrigatoriamente registradas no SICAF.

15. CONSIDERAÇÕES FINAIS.

15.1. Fica o presente Termo de Referência como esclarecedor de quaisquer dúvidas que por ventura venham a existir.

15.2. Nenhum pagamento será efetuado ao Contratado, enquanto pendente de liquidação, qualquer obrigação financeira que lhe for imposta em virtude de penalidade ou inadimplência, sem que isso gere direito ao pleito de reajustamento de preços ou correção monetária.

15.3. É condição do valor constante de cada nota fiscal/fatura, a apresentação de prova de regularidade com o Fundo de Garantia por Tempo de Serviço (FGTS), com o Instituto Nacional de Seguro Social (INSS), Certidões Negativas de Tributos, Estadual, Federal e Municipal e Certidão Negativa de Débitos Trabalhistas, conforme e determina normas legais que regem o caso.

Porto Velho, 01 de Outubro de 2019.

Termo de Referencia Elaborado por:
Bruno Jorge Sousa de Melo
Assessor de Tecnologia da Informação

Revisado por:
Tomaz Oliveira Mateus
Assessor de Coordenadoria

Autorizado por:
Eng. Ftal. Carlos Antônio Xavier
Presidente CREA/RO