	lista de da Prefeitura, portal da transparência, Ações referente a praias, árvores -- autorização para retiradas, árvores – plantio de mudas, árvores – retidas, balneabilidade, coleta seletiva, disque silêncio, fiscalização ambiental, licença ambiental, praças, construção e reconstrução de moradias, denúncia servidor, fala Pindoretama, agendamento online de serviços da saúde, controle de pragas em geral, defesa civil, emergência guarda municipal, emergência guarda de transito, internet pública, expansão de iluminação púlbica, fiscalização de vias públicas, fiscalização de transporte clandestino, atendimento ao turista de Pindoretama; Módulo de teleatendimento nativo no aplicativo, com, no mínimo, as funções: Área exclusiva do paciente integrada ao aplicativo da prefeitura de modo transparente, onde ele pode visualizar suas próximas consultas, com acesso à sala de atendimento num único clique; Deverá possuir um Portal de Serviços da Prefeitura onde terá informações sobre a história cidade, pontos turísticos e as notícias publicadas no portal da Prefeitura, além de disponibilizar uma gestão de serviços úteis a população, tais como: transportes, locais, andamento das obras, portal da transparência etc; Possuir funcionalidade para enviar e-mail aos principais setores da Prefeitura Municipal de Pindoretama, incluindo o gabinete do prefeito; Estar integrado ao Sistemas existentes para abertura de processos eletrônicos na Prefeitura Municipal de Pindoretama; Possibilitar acessar serviços disponibilizados no Portal Oficial do Município, tais como: Legislação Municipal, Diário Oficial, lista telefônica, emissão de notas fiscais, portal da transparência etc;. Possuir funcionalidade para agendamento de serviços especificando a categoria e serviço desejado; Feito a escolha do serviço desejado, dar ao cidadão as informações necessárias para o comparecimento, tais como: local, e documentos pessoais, com isso finalizando o agendamento; Possuir a funcionalidade para consultar o agendamento com algum documento do cidadão ou número do processo; Possuir modulo de gestão de projetos em execução que permite incluir fotos e informações sobre cada tipo de projeto da cidade.															
2	Link de internet dedicado 100% de banda garantida, com 500 MB de downloads, 500 MB de upload com instalação física e lógica com fornecimento de kit de instalação completo.	Unid	2	3	4	3	3	3	1	55	40	3	1	4	122
3	Link de internet móvel de 500 Mbps de downloads e 500 Mbps de uploads com instalação física e lógica e fornecimento de kit de instalação completo configurado para intranet Municipal (rede de dados, , imagem e aplicativo para estrutura itinerante direcionado para eventos(lives) da Prefeitura de Pindoretama que deve conectar em todos os bairros do Município.	Unid										1			1
4	Link de internet dedicado 100% de banda garantida, com 1 GB de downloads, 1 GB de upload, com firewall, destinado aos pontos de acesso público, incluindo instalação e configuração de hotspots.	Unid							14						14
															138

5.1. DESCRITIVO TÉCNICO DOS ITENS – EXIGÊNCIAS TÉCNICA MÍNIMA DOS EQUIPAMENTOS

5.2 - OLT

✓ Deverá ser um equipamento GPON "carrier class" de alta capacidade,que fornece um máximo de 8.192 ONUs, utilizando splitter com razão 1:64.

✓ Ao configurar os diferentes tipos de cartões,os usuários GPON e EPON podem estar conectados simultaneamente no mesmo chassi OLT.
✓ Está em conformidade com padrões internacionais,tais como o conjunto de normas ITU-T G.984 e IEEE 802.3ah e recomendações relacionadas.
✓ Por meio de diferentes tipos de ONU, implementa soluções FTTH / FTTB / FTTC para atender vários tipos de necessidades.
✓ Backplane do chassi com 10Gbps e do tipo "non traffic block";
✓ Suporta até 4 portas 10GE / 12 portas 1GE como uplinks,para conexão ao backbone da rede;
✓ Suporta um máximo de 8.192 ONUs por chassi
✓ Oferece economia de espaço devido ao tamanho compacto para sua classe de solução
✓ O chassi é projetado para ter confiabilidade "carrier class",semelhante a uma estrutura doublefabric. Os principais componentes do chassi podem ser configurados para redundância 1+1,inclusive para entrada de alimentação elétrica. Os mecanismos de proteção pode ser implementados no módulo ou entre módulos GPON.
✓ Todos os equipamentos FTTx GPON/EPON podem ser gerenciados por uma plataforma única.
✓ Dimensões (L×P×A mm): 480 × 270 × 621,5
✓ Peso do chassis : 40kg (com todos os módulos)
✓ Capacidade (Por cahssi/subrack): Suporta um máximo de 8.192 ONUs
✓ Capacidade (Por módulo de serviço): 4 ou 8 portas PON por módulo de serviço
✓ Capacidade do "Core Switch": 1000Gbps
✓ Temperatura de operação -10□ ~50□
✓ Temperatura de armazenamento -30□ ~65□
✓ Humidade do ambiente 5%~95%
✓ Serviços Ethernet
✓ Serviços CATV
✓ NGN (MGCP/H.248/SIP)
✓ Serviços TDM
✓ Serviço de broadcast de IPTV
✓ VOD unicast (Video On Demand)
✓ Até 4x portas ópticas ethernet 10 Gbps com XFP
✓ Até 12x portas ópticas ethernet 1Gbps com SFP
✓ Até 12× portas UTP/RJ45 ethernet 1 Gbps
✓ Até 128× portas E1
✓ Até 8× porta STM-1
✓ Porta GPON em conformidade com "Class B+,C" para ODN
✓ Porta EPON 1000BASE-PX10/PX20 para ODN
✓ Alcance máximo de até 20km
✓ Conector SC/PC
✓ Suporta fibra de núcleo único G.652/G.657
✓ Comprimento de onda: TX 1490nm(1550nm)/RX 1310nm
✓ Taxa de recepção(Upstream)/trasmissão(Downstream): 1,244Gbps/2,488Gbps para GPON
✓ Taxa de recepção(Upstream)/trasmissão(Downstream): 1,25Gbps/1,25Gbps para EPON
✓ Duas entradas para fontes de alimentação em cada chassi/subrack
✓ Dois módulos de controle por chassi/subrack
✓ Dois módulos de uplink por chassis/subrack
✓ Mecanismo de proteção entre as portas PON
✓ Potência consumida configuração completa: 850W (com todos os módulos)
✓ Fonte de alimentação: -48V DC (-40V~-57V)

Comissão de Licitação
Folha Nº
277

5.3 - Cordão de Fibra Óptico

✓ Cordão Fibra Optico Sc/apc-Sc/upc Sm 2,0mm 9/125 Patchcord.
✓ Características. Conector: SC e LC. Polimento: UPC ou APC; Modelo: Simplex,monomodo;
✓ Especificações técnicas. Cor do conector: Azul (SM SC/UPC) / Verde (SM SC/APC) Perda de retorno: > 50dB (SM SC/PC) / > 60dB (SM SC/APC/APC) > 30dB (MM SC/PC);

5.4 – DIO

Desenvolvido para concentração, acomodação, distribuição e fusão de fibras ópticas. Instalado em racks de 19" ou 23" (rotação do suporte de fixação), o modelo FIT permite a acomodação de até 24 fusões em bandejas sobrepostas e articuladas ocupando apenas 1U de altura. Possibilita a utilização de cabos internos ou externos, com fibras monomodo (SM) ou multimodo (MM) do tipo loose, tight ou multicordão. Possui gaveta deslizante e painel de adaptadores intercambiável, que permite a fixação

de adaptadores LC, SC, E2000, ST ou FC. Estrutura externa confeccionada em aço carbono SAE 1010 com espessura de 1,2mm COMPOSIÇÃO Tampa frontal em aço carbono SAE 1010 com espessura de 0,9mm Bandejas internas em plástico de engenharia na cor branca

5.5 – CTO (Caixa de Terminação Óptica)

É utilizada para acomodação e proteção necessária para a construção da rede óptica FTTx. Comporta a terminação do cabo backbone para conectar com o cabo drop low friction na rede. A CTO 0216 possibilita emendas, divisão e distribuição de fibras.

- ✓ Possui suporte para sangria de cabo;
- ✓ Estrutura com travas de fechamento;
- ✓ Material: PC+ABS, à prova de umidade, água, poeira e antienvelhecimento;
- ✓ Grau de proteção: IP55;
- ✓ Adequada para uso indoor e outdoor;
- ✓ Ideal para uso em posição vertical: parede ou poste;
- ✓ Permite aterramento;
- ✓ Painel para 16 adaptadores ópticos SC;
- ✓ Permite conexão de splitter óptico mini module 1×4, 1×8 ou 1×16;
- ✓ Suporte para cabos ópticos;
- ✓ Suporte para emenda óptica;
- ✓ Produto com homologação Anatel.

5.6 - CEO (Caixa de Emenda Óptica)

✓ É utilizado para proteção e acomodação de emendas ópticas para transição ou derivação entre cabos de fibra óptica. Aplicável em vias aéreas com capacidade para até 36 fibras. Possui capacidade de até 12 emendas ópticas por bandeja e permite derivações e terminação dos cabos ópticos. Configuração tipo "topo" e sistema de vedação termocontrátil.

- ✓ Dimensões compactas;
- ✓ Fechamento e vedação com O'ring;
- ✓ Possibilidade de fechamento com cadeado;
- ✓ Possui bandeja para reserva de fibra com tubo "loose";
- ✓ Sistema de acomodação: áreas separadas para armazenar, encaminhar, proteger e "transportar" as fibras;

5.7 – Placa de Identificação Óptica

✓ Utilizados na identificação de cabos ópticos. Fabricadas em material termoplástico de alta resistência e durabilidade, contendo em sua composição aditivos que protegem o produto contra as ações nocivas dos raios UV. Dimensões (mm):Altura: 40mm;Largura: 90mm;Espessura: 3mm;

5.8- Cabo de Fibra Drop

✓ O Cabo Drop é utilizado em redes ópticas FTTH para instalações para o usuário final. Sua estrutura é composta por fibra de baixa sensibilidade a curvatura do tipo G.657, que possibilita um raio de curvatura menor e com níveis baixos de atenuação. Utiliza revestimento externo anti-UV, baixa emissão de fumaça e gases tóxicos sem halogênios (LSZH). Possui elementos de tração em aço, que possibilita sua instalação em dutos sem utilização de guia, e também o elemento de sustentação em aço que possibilita a instalação aérea. Com sua composição compacta, é ideal para aplicação no acesso ao assinante em redes ópticas internas/externas (FTTH), reduzindo o investimento em acessórios para sua instalação por ser um cabo auto-sustentado.

- ✓ Membro de forca 2x cabo de aço 0,45m
- ✓ Medidas Dimensão 5,2(±0,2)*2,0(±0,2)mm;
- ✓ Modelo Material LSZH;
- ✓ Cor Preto.

5.9 - Conector Fast APC

- ✓ Conector reutilizável sem perda de características;
- ✓ Pré-polimento APC;
- ✓ Montagem simples e rápida;
- ✓ Tempo de instalação inferior 3 min;
- ✓ Baixa Perda de inserção ≤ 0.3dB;
- ✓ Perda do retorno: ≥ – 40dB;
- ✓ Taxa de reflexão: ≥ 45 ~ 53dB;
- ✓ Temperatura de Operação: – 40 ~ +75°C.

5.10 - Conector Fast UPC

- ✓ Conector reutilizável sem perda de características;

- ✓ Pré-polimento UPC;
- ✓ Montagem simples e rápida;
- ✓ Tempo de instalação inferior 3 min;
- ✓ Baixa Perda de inserção ≤ 0.3dB;
- ✓ Perda do retorno: ≥ – 40dB;
- ✓ Taxa de reflexão: ≥ 45 ~ 53dB;
- ✓ Temperatura de Operação: – 40 ~ +75°C.

5.11 – ONU (Optical Network Unit)

✓ É o equipamento instalado no usuário que recebe o sinal transmitido pela OLT. O modelo AN5506-02-B possui uma porta Giga, uma porta Fast Ethernet e uma porta FXS (POTS), design discreto e é de fácil configuração atendendo todas as necessidades de serviços dos usuários finais. Ele oferece aos usuários serviços de comunicação e entretenimento na forma de dados, , vídeo, entre outras características, para satisfazer a procura de acesso integrada na sua casa ou empresa.

- ✓ Interface de interface de rede GPON
- ✓ Fonte de alimentação DC: 12 V / 1 A
- ✓ Potência <5W
- ✓ Proteção contra raios
- ✓ Temperatura de operação -5°C a 45°C
- ✓ Humidade ambiente 10% a 95% (sem condensação)
- ✓ Suporta o padrão IEEE 802.1Q VLAN.
- ✓ Suporta juntar a VLAN 802.1Q no modo / untag.
- ✓ Suporta até 4095 VLANs.
- ✓ Suporta o protocolo IGMP Snooping.
- ✓ Suporta IGMP v1 / v2 / v3.
- ✓ Encaminhamento de velocidade:
- ✓ Suporta o encaminhamento de fio-velocidade de Camada 2 / Camada 3.
- ✓ Suporta a pilha dupla IPv4 / v6.
- ✓ Suporta filtragem de pacotes, filtragem de endereço MAC e filtragem de URL.
- ✓ Suporta proteção contra ataques ilegais (DoS, ARP); Suporta tempestades de broadcast de supressão.
- ✓ Suporta a obtenção do endereço IP do usuário no modo DHCP; Suporta o relatório da localização física da interface Ethernet usando DHCP Option82.
- ✓ Suporta a obtenção do endereço IP do usuário no modo PPPoE; Suporta a função PPPoE +, usada para identificar usuários precisos Suporta criptografia de dados de downlink nos o algoritmo AES-128.
- ✓ Suporta a função ACL para corresponder tráfego com base nas regras ACL.
- ✓ Suporta configuração global de prioridade de fila e mapeamento flexível de valores 802.1p em pacotes.
- ✓ Suporta três modos de agendamento de filas (PQ, WRR e PQ + WRR); Suporte à configuração do peso do, De modo a garantir a qualidade do serviço de alta QoS serviços, tais como e vídeo no ambiente multi-serviço.
- ✓ Interface GPON
- ✓ Fornece uma interface GPON (interface SC / UPC ou SC / APC), suportando uma distância de transmissão de até 20 km cumprindo a norma ITU-T G.984.
- ✓ Suporta Classe B +, com sensibilidade de recepção inferior a -29 dBm.
- ✓ Interface LAN
- ✓ Fornece duas interfaces LAN (interfaces RJ-45), suportando full-duplex ou halfduplex e 10/100/1000 Mbit / s auto negociação. A distância máxima de transmissão é de 100 m.
- ✓ Capacidade de endereço MAC: 1K
- ✓ Fornece uma interface de (interface RJ-11).
- ✓ Tipo de Aplicação: Interna (Indoor)
- ✓ Tamanho em mm (AxLxP): 25,5x112x112
- ✓ Peso: 0,12 kg
- ✓ Temperatura de operação: -5°C ~ 45°C
- ✓ Humidade: 10% ~95% não condensado
- ✓ Interface de Serviço: 1 portas Gigabit Ethernet – GE
- ✓ Consumo de Alimentação: 4 Watts
- ✓ Fonte de Alimentação: DC 12V

5.12- Roteador Wifi 4 Antenas Dual Band Wireless Ac 1200mbps

✓ Possuir a tecnologia Wi-Fi 5 (802.11ac), popularmente chamada de dual band AC 1200), contando com velocidade de até 867Mbps em 5 GHz e 300Mbps em 2,4 GHz.Tem ainda suporte a

Beamforming e MU-MIMO, garantindo uma navegação mais veloz e estável mesmo com mais dispositivos conectados na rede Wi-Fi.Através de suas 3 portas LAN Fast Ethernet (10/100Mbps) é possível usufruir de conexão de qualidade também através da rede cabeada. Além disso, é compatível com o Portal Remotize, que simplifica o gerenciamento do parque de roteadores, por exemplo, permitindo atualização de firmware e customização de configurações-padrão de forma centralizada.4 portas fast (1 Internet e 3 LAN).

✓ Customização de configurações-padrão via Portal Remotize: evite visitas a campo, por exemplo, em caso de reset

✓ Atualização remota centralizada via Portal Remotize: mantenha seu parque de roteadores sempre atualizado, de forma prática e fácil

✓ Tecnologia Wi-Fi 5 com até 867Mbps em 5 GHz (802.11ac) e 300Mbps em 2,4 GHz (802.11n)

✓ Suporte a Beamforming e MU-MIMO: maior performance e estabilidade mesmo com mais dispositivos conectados na rede Wi-FiSuporte a IPv6: seu parque de roteadores pronto para o mais recente protocolo de internet.

Comissão de Licitação
Folha Nº
280

5.13 4 antenas externas fixas de 5 dBi

✓ 4 portas Fast Ethernet – 1 WAN e 3 LAN – 10/100 Mbps
✓ LEDs: Power, Internet, LAN, Wi-Fi 2,4 GHz, Wi-Fi 5 GHz
✓ Chipset Realtek® RTL8197FH-VG4-CG + RTL8812FR-CG
✓ Memória Flash 8 MB Memória RAM 64 MB
✓ Botão RESET/WPS (importante: produto não possui WPS habilitado)
✓ SO Linux + Bifrost Intelbras
✓ Compatível com plataforma Remotize
✓ Padrões IEEE 802.11a/b/g/n/ac Modo do rádio MU-MIMO, Beamforming Modo de operação Roteador Frequência de operação 2,4 GHz / 5 GHz Largura de banda 2,4 GHz: 20, 40 MHz com coexistência habilitada por padrão 5 GHz: 20, 40, 80 MHz Taxa de transmissão 2,4 GHz: até 300 Mbps / 5 GHz: até 867 Mbps Canais de operação 2,4 GHz: 1-13 (Brasil) / 5 GHz: 36, 40, 44, 48, 149, 153, 157, 161 Potência máxima (E.I.R.P.) 2,4 GHz (n40 MCS7): 250 mW (24 dBm) / 5 GHz (ac80 MCS9): 200 mW (23 dBm) Sensibilidade de recepção em 2.4 GHz -76dbm@802.11b -68dbm@802.11g -65dbm@802.11n 20MHz MCS7 -62dbm@802.11n 40 MHz MCS7 Sensibilidade de recepção em 5 GHz -72dbm@802.11a -69dbm@802.11n 20MHz MCS7 -65dbm@802.11n 40MHz MCS7 -63dbm@802.11ac 20MHz MCS8 -57dbm@802.11ac 40MHz MCS9 -54dbm@802.11ac 80MHz MCS9 Segurança WPA-WPA2/PSK com criptografia AES FONTE DE ALIMENTAÇÃO Entrada 100-240 V a 50/60 Hz Saída 12 Vdc/1 A Potência de consumo máxima 12 W

✓ **5.14 - Roteador Wifi Praca com Antena**

✓ Deve possuir Processador Qualcomm Atheros ARM v7 Largura de Canal 5, 10, 20, 40 Mhz. Padrão Compatibilidade 802.11b,g,n, Wi-Fi com total compatibilidade MIMO Recurso MESH (Gerenciável) Equipado com STP - Spinning Tree Protocol (anti TCP/IP looping) Modos b, g, n Velocidade Até 300Mbps Frequência 2.412GHz ~ 2.484GHz Potência Agregada 800mW (29dBm) Sensibilidade Até - 102dBm -Alta Seletividade Multi SSID Até 16 SSIDs c/ configuração individual de segurança/acesso Até 254 Conexões Simultâneas Smart roaming automático Até 5 Modos de Operação: Access Point, Access Point Gateway (Router), Client/Station, AccessPoint WDS (repeater), Client/Station WDS (client de repeater) Suporte para até 4092 VLANs Segurança desligada, WEP Open System, WEP Shered Key, WPA-PSK, WPA2-PSK, WPA-PSK/WPA2-PSK Mixed Mode, WPA-EAP, WPA2-EAP, IEEE802.11x (Radius - Para até 2 servidores). Controle de Banda Coletivo ou individual p/usuário QoS 802.11e, WMM (prioriz.de dados, e imagem). Ethernet interface 10/100/1000 BASE-TX Fast Recurso Video Over Wireless - VoW Tecnologia ADT (Active Diversity Technology) Hotspot Gerenciável - Via Servidor externo. Gráficos e Estatísticas Diversas Realtime Load, Realtime Traffic, Realtime Wireless, e Realtime Connections. Gerenciamento Individual Via HTTP, HTTPS, SSL, Telnet e SNMP Gerenciamento Centralizado via Allied Stratus Controller Monitoramento Online Via Stratus Floorplan Alimentação Elétrica 12 a 24VDC@8W (PoE) 802.3af (Passivo) Proteção contra descargas Elétricas ESD/EMP 15 KeV

✓ **5.15 - Monitor LCD 15"**

✓ Tamanho mínimo da Tela: 15"
✓ Tipo de tela: LCD
✓ Entrada: DVI e VGA/RGB
✓ Relação de Aspecto: 16:9 ou 16:10 (Widescreen)
✓ Resolução: 1680 x 1050
✓ Contraste Ratio: acima de 10000:1

5.16 - Rack para NGC com Acessórios

✓ Deve cumprir a norma EIA310-D; Construção em perfis 19 polegadas, extremamente reforçados, com diversos pontos de fixação por perfil, compatíveis com os servidores comercializados no mercado,

ajustáveis na profundidade sem uso de ferramentas; Espaço para interconexões, frente 85,5mm; Capacidade de carga mínima de 400 kg quando acoplados, incluso o peso do rack; Capacidade de proteção IP20; Teste de Vibração de acordo conforme MIL-STD 810 E; Estrutura básica em alumínio extrudado e polido; Teto com flanges para entrada de cabos laterais, flanges para instalação opcional de ventiladores, e perfurações para ventilação natural; 148. Pés niveladores com capa de borracha;

- ✓ Bandeira para rack 44U, 44 x 770 fixa de cor preta.
- ✓ Calha pra rack 19" com 08 tomadas cor preta 20A.
- ✓ Guia de cabos fechados 1Ux80x19, cor preta
- ✓ Porta Gaiola Completo.
- ✓ Mouse Óptico PS2.
- ✓ Teclado PS2.
- ✓ Chaveador KVM Controla 8 Computadores, Modo Auto-Scan e display de LED para monitoramento de PCs, Status do teclado restaurado quando chaveia PCs, Som de bip para confirmação de troca de porta, Seleção de PCs via operação Hot-Key ou push button, Plug & Play e Hot-Pluggable, Arquitetura de Montagem em rack EIA-19 (1U), Interfaces e Conexões de Entrada (no Console): 1x PS/2 (Fêmea - p/ mouse), 1x PS/2 (Fêmea - p/ teclado), 1x VGA (HDB - 15 pinos - Fêmea), Interfaces e Conexões de Saída (no Console): 8x PS/2 (Fêmea - p/ mouse), 8x PS/2 (Fêmea - p/ teclado), 8x VGA (HDB - 15 pinos - Fêmea), Resolução de vídeo (máx.): 1.920 x 1.440, Adaptador de energia:Entrada: 100 ~ 240V / 50 - 60Hz.

5.17 - Servidor Cloud Core Router

- ✓ CPU frequência nominal de 1 GHz
- ✓ CPU contagem de núcleos 72
- ✓ Tamanho de RAM 16 GB
- ✓ De armazenamento de 128 MB Onboard NAND, veja também a expansão
- ✓ 10/100/1000 portas Ethernet 1
- ✓ Fonte de alimentação 2x IEC C14 conectores padrão 110 / 220V (Two PSU redundante)
- ✓ Compatível tensão de entrada de 12 V
- ✓ monitor de temperatura CPU Sim
- ✓ monitor de temperatura PCB Sim
- ✓ Voltage Monitor de Sim
- ✓ monitor atual Sim
- ✓ Dimensões 443x315x40mm, peso: 3,8 kg, peso com embalagem: 5.125 kg
- ✓ nível de licença 6
- ✓ RouterOS sistema operacional
- ✓ CPU Tilera Telha-Gx72 CPU
- ✓ Consumo Máximo de Energia 100 W
- ✓ Display LCD a cores, touchscreen+ gaiolas SFP 8x 10G Ethernet SFP (Mini-GBIC; módulo SFP não incluído), suporte CMSDExpansão 1x microUSB 2.0, 1x USB regulares 2.0, tamanho completo Smart Card entalhe, slot microSD,2x M.2 slots com PCIe x4 2.0, Key-M, o apoio tamanho do módulo: 2242,2260,2280 porta serial RJ45.

5.18 - Software para Gerenciamento de Rede

- ✓ O sistema de gerenciamento deve ser em conformidade com a especificação deste Edital;
- ✓ Deve ser compatível com a plataforma Microsoft Windows e Linux;
- ✓ O sistema deve possuir licenças suficientes para permitir o gerenciamento de todos os equipamentos ofertados, sendo que cada equipamento poderá ter vários itens gerenciáveis, tais como portas, objetos da MIB, etc;
- ✓ Permitir atualização de versões de software;
- ✓ Funcionar sem a necessidade de um framework de gerência de terceiros;
- ✓ Possuir interface gráfica que permita a gerência, configuração e suporte a todos os equipamentos contidos na proposta, utilizando MIBs padrão e MIBs proprietárias;
- ✓ Possuir interface gráfica de gerenciamento Web seguro (HTTPS);
- ✓ Prover detecção automática da topologia da rede;
- ✓ Permitir a apresentação gráfica da topologia da rede, mostrando os equipamentos e suas interligações.
- ✓ Permitir o recebimento e interpretação de traps;
- ✓ Possibilitar a definição de thresholds, além de disparar alarmes e notificações (via e-mail) quando um determinado threshold definido pelo usuário for atingido;
- ✓ Na representação gráfica da rede, deverá ser permitida a identificação, por graduação de cores, dos diferentes níveis de severidade de falhas dos equipamentos e o diagnóstico do estado do equipamento.
- ✓ Monitorar o estado de todas as portas dos equipamentos;

✓ Permitir a ativação e desativação das portas dos equipamentos;
✓ Permitir localização automática da porta onde está conectado um determinado endereço IP ou MAC;
✓ Implementar servidor de "Syslog";
✓ Possuir ferramentas de inventário de software e hardware dos equipamentos;
✓ Permitir backup da base de dados da solução de gerenciamento;
✓ Permitir backup programado da configuração dos equipamentos;
✓ Permitir distribuição e instalação de softwares e scripts de configuração para os equipamentos;
✓ Possibilitar procedimentos de gerenciamento e configuração de VLANs, tais como a visualização, criação, reconfiguração, remoção e distribuição automática de configurações aos equipamentos envolvidos, sem que seja necessário o acesso individual a cada um desses equipamentos;
✓ Ser compatível com SNMPv1, SNMPv2, SNMPv3 e RMON 1 (ou NetFlow ou Sflow) e permitir o tratamento de informações pertinentes a estes padrões;
✓ Permitir a coleta de informações estatísticas de todos os switches ofertados para a solução;
✓ Permitir a inclusão de novas MIBs na plataforma de gerenciamento, em conformidade com os padrões SNMP;
✓ Possibilitar a implementação e o gerenciamento de políticas de QoS ("Quality of
✓ Service"), bem como permitir a criação, modificação, visualização, remoção e distribuição automática de políticas aos equipamentos envolvidos, sem que seja necessário o acesso individual a cada um desses equipamentos;
✓ Exigir senha para acesso ou alteração da configuração;
✓ Possuir ferramenta de geração de relatórios personalizados;

5.19 - Servidor de Appliance Unificado de Segurança

✓ Solução integrada de segurança da informação do tipo UTM (Unified Threat Management) que tenha a capacidade de integrar em um único dispositivo: filtro de pacotes com controle de estado, filtro de conteúdo WEB, filtro anti-spam, VPN, IDS/IPS, balanceamento de carga, QoS e Proxy reverso.

✓ **REDE:**

✓ Efetuar controle de tráfego por estado no mínimo para os protocolos TCP, UDP e ICMP baseados nos endereços de origem, destino e porta;
✓ Suportar o Internet Protocol Versões 4 e 6 (IPv4 e IPv6);
✓ Suportar o protocolo 802.1q, para uso e segmentação da rede com VLANs;
✓ Capacidade para trabalhar com conversão de endereços e portas (NAT/NAPT) conforme RFC 3022;
✓ Suportar no mínimo os seguintes protocolos de roteamento dinâmico: RIP1, RIP2 e OSPF;
✓ O equipamento deverá suportar o registro do dispositivo dinamicamente, pelo seu endereço IP de WAN, em pelo menos 5 (cinco) provedores de serviços de DDNS;
✓ Possuir mecanismo de forma a possibilitar o funcionamento transparente dos protocolos FTP, Real Áudio, Real Vídeo, RTSP, H.323 e PPTP mesmo quando acessados por máquinas através de conversão de endereços. Este suporte deve funcionar tanto para acessos de dentro para fora quanto de fora para dentro;

✓ **AUTENTICAÇÃO:**

✓ Prover autenticação de usuários para os serviços Telnet, FTP, HTTP, HTTPS e Gopher, utilizando as bases de dados de usuários e grupos de servidores Windows e Unix, de forma simultânea;
✓ Permitir a utilização de LDAP, LDAP/SSL, LDAP/TLS, RADIUS, hardware tokens (SecureID ou equivalente), certificados X.509 (gravados em disco e/ou em tokens criptográficos/smartcards) e sistema S/KEY para a autenticação de usuários;
✓ Permitir o cadastro dos usuários e grupos em base de dados própria por meio da interface de gerencia remota do dispositivo;
✓ 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 (Certificates Revogation Lists) emitidas periodicamente pelas autoridades, que devem ser obtidas automaticamente pelo dispositivo via protocolos HTTP e LDAP;
✓ Permitir o controle de acesso por usuário, para plataformas Windows NT, 2000, 2003, 2008, XP, Vista e Windows 7 de forma transparente (sem a necessidade do usuário digitar novamente a senha), para todos os serviços suportados, de forma que ao efetuar o logon na rede, um determinado usuário tenha seu perfil de acesso automaticamente configurado;
✓ Possuir perfis de acesso hierárquicos;
✓ Permitir a atribuição de perfil de acesso a usuário ou grupo de usuários de acordo com o endereço ou range IP do equipamento que o usuário esteja utilizando;

✓ **POLÍTICA DE TRÁFEGO:**

✓ Permitir o agrupamento das regras de filtragem por política;

Comissão de Licitação
Folha Nº 282

✓ Prover mecanismo que permita a especificação de datas de validade inicial e final, para regras de filtragem, individualmente (por regra);
✓ Prover mecanismo que permita a especificação da validade para regras de filtragem, individualmente (por regra), por dia da semana e horário;
✓ Permitir a visualização em tempo real de todas as conexões TCP e sessões UDP ativas através do dispositivo e a finalização 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 dado momento;
✓ 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 mecanismo que permita capturar o tráfego de rede em tempo real (sniffer) via interface gráfica, com capacidade para exportação dos dados capturados para arquivo no mínimo em formato PCAP;
✓ Permitir configuração de filtros para a captura do tráfego em tempo real, no mínimo por protocolo, endereço IP de origem e/ou destino e porta de origem e/ou destino, utilizando para tanto linguagem textual;
✓ Permitir a visualização do tráfego de rede em tempo real (sniffer) tanto nas interfaces de rede do dispositivo quando nos pontos internos do mesmo: anterior e posterior à filtragem de pacotes, onde o efeito do NAT/NAPT
✓ (tradução de endereços) é eliminado; o Permitir a execução de até oito capturas de tráfego em tempo real simultaneamente, inclusive em pontos diferentes ou com filtros diferentes;
✓ **SEGURANÇA:**
✓ Prover mecanismo contra ataques de falsificação de endereços (IP Spoofing) através da especificação da interface de rede pela qual uma comunicação deve se originar;
✓ Prover proteção contra os ataques de negação de serviço SYN Flood, Land, Tear Drop e Ping O'Death;
✓ Possuir mecanismo que limite o número máximo de conexões simultâneas de um mesmo cliente para um determinado serviço e/ou servidor;
✓ Detectar automaticamente e inserir regras de bloqueio temporárias para varreduras de portas efetuadas contra o dispositivo ou contra qualquer máquina protegida por esse, mesmo que realizados em períodos maiores que 1 (um) dia;
✓ Permitir integração com sistema detecção de intrusão (IDS) externo, permitindo que esses agentes insiram regras temporárias no dispositivo em caso de detecção de algum ataque, com duração pré-determinada, de forma automática;
✓ Possuir sistema de prevenção de intrusão (IPS) nativo, permitindo o bloqueio do ataque em caso de detecção do mesmo;
✓ Possuir filtro de aplicações de modo a permitir a identificação de padrões de dados dentro das conexões, possibilitando o tratamento automático (bloqueio, liberação ou redução/aumento de banda) de aplicações do tipo peer-to-peer, de download de arquivos, entre outros;

✓ **MONITORAMENTO E ADMINISTRAÇÃO:**
✓ Possuir suporte ao protocolo SNMP (v1, 2 e 3) através de MIB2;
✓ Permitir em tempo real a visualização de estatísticas do uso de CPU, memória do dispositivo, bem como o tráfego de rede em todas as interfaces do dispositivo através da interface gráfica remota, de forma gráfica ou em tabelas;
✓ Caso o dispositivo utilize agentes externos para divisão de processamento (antivírus, filtro de conteúdo, IDS ou Anti-spam) o dispositivo deverá permitir a verificação em tempo real da comunicação com estes agentes;
✓ Possuir sistema de alerta que informe o administrador através de e-mails, janelas de alerta na interface gráfica, execução de programas e envio de traps SNMP;
✓ Permitir a criação de perfis de administração baseado em papéis (role-based), de forma a possibilitar a definição de diversos administradores para o dispositivo, cada um responsável por determinada tarefa da administração;
✓ Permitir a conexão simultânea de vários administradores, sendo apenas um deles com poderes de alteração de configurações e os demais apenas de visualização das mesmas;
✓ Permitir que o segundo administrador ao se conectar possa enviar uma mensagem ao primeiro através da interface de administração;
✓ Fornecer gerência remota, com interface gráfica nativa, através de canal criptografado com chave de criptografia igual ou superior a 128 bits, para plataformas Windows Me, Windows NT/2000/XP/2003/2008/Vista/Windows 7,

Comissão de Licitação
Folha Nº
283

✓ Linux;
✓ Capacidade para criação de entidades/objetos, que podem ser um IP, um range IP ou um dispositivo, etc. para facilitar a administração;
✓ Possibilitar drag-and-drop (arrastar e soltar) para criação e alteração de regras, por meio da interface gráfica;
✓ A interface gráfica deverá possuir mecanismo que permita a gerência remota de múltiplos dispositivos sem a necessidade de se executar várias interfaces;
✓ A interface gráfica deverá possuir assistentes para facilitar a configuração inicial e a realização das tarefas mais comuns na administração do dispositivo, incluindo a configuração de VPNs, NAT, perfis de acesso e regras de filtragem;
✓ Possuir mecanismo que permita a realização de cópias de segurança (backups) e restauração remota, através da interface gráfica, sem necessidade do reinício do sistema;
✓ o Possuir mecanismo que possibilite a aplicação de correções e atualizações para dispositivo de forma remota por meio da interface gráfica;
✓ Possuir mecanismo anti-suicídio para a administração remota, evitando que o administrador perca o acesso ao dispositivo por uma configuração incorreta;
✓ Permitir de integração com produto de gerenciamento centralizado de múltiplos dispositivos;
✓ Possuir interface orientada a linha de comando (Command Line Interface) para a administração do dispositivo a partir do console;
✓ Suportar o rollback (voltar para a versão anterior) de patches aplicados;
✓ LOG:
✓ Prover mecanismo de consulta às informações registradas (logs) por meio da interface gráfica de administração;
✓ Possibilitar o armazenamento de seus registros (log e/ou eventos) em máquina remota em plataformas Windows Server (NT/2000/2003/2008) ou Unix, através de protocolo criptografado ou SYSLOG;
✓ **RELATÓRIOS:**
✓ Possibilitar a geração de pelo menos os seguintes tipos de relatório, publicados em formato HTML:
✓ Máquinas mais acessadas;
✓ Serviços mais utilizados;
✓ Usuários que mais utilizaram serviços;
✓ URLs mais visualizadas;
✓ Categorias Web mais acessadas (em caso de existência de um filtro de conteúdo Web);
✓ Maiores emissores/receptores de e-mail;
✓ 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 (quando utilizado com filtragem de conteúdo Web);
✓ Possibilitar a geração dos relatórios dos dois itens acima sob demanda e através de agendamento diário, semanal e mensal;
✓ Permitir publicação automatizada dos relatórios utilizando FTP em pelo menos três equipamentos distintos;
✓ Permitir exportação dos logs no mínimo em formato TXT e CSV;
✓ QOS:
✓ Implementar mecanismo de divisão justa de largura de banda (QoS), permitindo a priorização de tráfego por regra de filtragem, por usuário ou ainda priorizando acesso a sites por categoria ou palavra-chave;
✓ Implementar mecanismo de limitação de banda através da criação de canais virtuais, permitindo que os mesmos serem alocados por regra de filtragem e por usuário;
✓ Permitir modificação (remarcação) de valores DSCP para o DiffServ;
✓ Implementar no mínimo 07 classes de serviço distintas, com configuração do mapeamento e marcação para códigos DSCP através da interface gráfica;
✓ Possuir suporte ao protocolo SNMP (v1, 2 e 3), com MIB2;
✓ Suportar o uso simultâneo de múltiplos links em um mesmo firewall, de provedores distintos ou não, sendo o firewall o responsável por dividir o tráfego entre os distintos links;
✓ Permitir o balanceamento de links com IPs dinâmicos para ADSL, ou outra tecnologia de banda larga que não utilize IP Fixo;

Comissão de Licitação
Folha Nº
284

✓ **BALANCEAMENTO:**

✓ Implementar mecanismo de balanceamento de carga, permitindo com que vários servidores internos, sejam acessados externamente pelo mesmo endereço IP. O balanceamento de canal deverá monitorar os servidores internos e, em caso de queda de um destes, dividir o tráfego entre os demais, automaticamente;

✓ Implementar mecanismo de persistência de sessão para o balanceamento de carga, através de diversas conexões, para quaisquer protocolos suportados pelos servidores sendo balanceados;

✓ O balanceamento de carga deverá ainda possibilitar que os servidores sejam monitorados através do protocolo ICMP ou requisições HTTP. Ele deverá também possuir pelo menos dois algoritmos distintos de balanceamento;

✓ Suportar a criação de clusters com tolerância a falhas, onde poderá trabalhar no mínimo de 2 formas, de acordo com a necessidade da instalação. Sendo elas:

✓ Os dois dispositivos são ligados em paralelo, com replicas do estado de conexões entre eles. O dispositivo secundário não estará tratando o tráfego, ele entrará em funcionamento para tratamento de tráfego somente quando o dispositivo principal cair, sem que se tenha perda de conexão ou de canal VPN;

✓ Dois ou mais dispositivos devem estar em funcionamento simultaneamente, balanceando o tráfego de rede entre eles de forma automática e replicando configuração e estado das conexões também de forma automática, sem que se tenha perda de conexão ou de canal VPN no caso de falha de algum equipamento. Nesta modalidade, podem ser colocados até 64 firewalls em paralelo;

✓ Sistema de Prevenção contra Intrusão para UTM:

✓ Possuir sistema de prevenção de intrusão (IPS) nativo, permitindo seja inseridas regras temporárias no firewall em caso de detecção de algum ataque, com duração pré-determinada, de forma automática;

✓ A base de assinaturas do sistema de IPS nativo deverá ser fornecida pelo período do contrato;

✓ Possuir filtro de aplicações de modo a permitir a identificação de padrões de dados dentro das conexões, possibilitando o tratamento automático (bloqueio, liberação ou redução/aumento de banda) de aplicações do tipo peer-to-peer, de download de arquivos, entre outros;

✓ Filtro de acesso WEB com atualização de URL's para UTM:

✓ Possuir capacidade para efetuar classificação de URLs, de maneira a bloquear acesso a páginas WEB, para usuários ou grupo deles, a partir de categorias genéricas;

✓ Possuir pelo menos 70 categorias de classificação de URLs a serem consultadas no analisador de URLs do item anterior;

✓ Deverão ser fornecidas todas as atualizações de software assim como a atualização da base de conhecimento (URLs categorizadas), sem custo adicional, por todo o período do contrato;

✓ Possuir documento do fabricante atestando que as classificações de URLs são realizadas de forma manual, ou seja, não são feitas através de palavras-chave, evitando dessa forma a ocorrência de classificações errôneas;

✓ Possibilitar agendamento mensal e semanal do download automático das atualizações das URLs;

✓ Possuir mecanismo que permita fazer download apenas das novas atualizações diárias e não da base completa, de modo a economizar banda do link com a Internet;

✓ Possui pelo menos 12.000.000 (Doze Milhões) de URLs classificadas;

✓ Filtro de detecção de SPAM bayesiano para UTM:

✓ Fornecimento de todas as atualizações de software assim como a atualização da base de conhecimento (novas regras de detecção de SPAM) por todo período do contrato;

✓ Deverá avaliar as mensagens e atribuir uma nota a cada uma delas, que corresponda à probabilidade da mesma ser SPAM, variando de 0 a 100%;

✓ As notas atribuídas às mensagens deverão ser calculadas utilizando-se bancos de dados com informações estatísticas obtidas de milhares de mensagens de email, e produzidas através de análise bayesiana;

✓ Os bancos de dados com informações estatísticas deverão poder ser atualizados diária e automaticamente, através de download via Internet;

✓ Deverá possuir dois modos distintos de atribuição de notas para as mensagens: um que prioriza a detecção de SPAM e outro que reduz os falso-positivos;

✓ Deverá possibilitar que os usuários realizem treinamento do banco de dados de mensagens informando, para cada mensagem recebida, se a mesma é ou não SPAM;

✓ Permitir a criação de bases de dados de classificação distintas para cada usuário ou grupo de usuários, a fim de que cada base represente um perfil de usuário ou grupo de usuários específicos;

✓ Permitir mecanismo que faça com que o treinamento de cada usuário seja aproveitado somente na base correspondente ao seu grupo ou usuário do sistema;

Comissão de Licitação
Folha Nº
285

✓ Permitir o backup e restauração das bases com os treinamentos dos usuários via interface de administração remota;
✓ Deverá possuir plugins para realização do treinamento das mensagens pelo menos para os clientes de e-mail Microsoft Outlook e Thunderbird;
✓ Deverá possuir mecanismo de treinamento de mensagens para os leitores de email para os quais não exista plugin disponível, através da modificação da mensagem original. Esta modificação deverá funcionar para qualquer cliente de
✓ e-mail que suporte a leitura de mensagens HTML;
✓ Possibilitar o registro de todas as classificações e treinamentos realizados através do servidor, e de todas as tentativas de abertura de sessões ou conexões que forem recusadas pelo mesmo;
✓ Possibilitar o registro de todas as operações envolvendo as bases de dados do sistema de detecção, tais como download, upload e recálculo;
✓ Possibilitar registro da remoção, restauração ou criação de backup de bases;
✓ Possuir mecanismo que permita a configuração do log (tempo de permanência das mensagens, tamanho de arquivo, etc) e visualização das mensagens de log através da interface gráfica;
✓ o Possibilitar o envio de registros para o sistema operacional (syslog no caso de sistemas UNIX e Event Viewer em Windows;
✓ O equipamento deve se instalar em rack com largura padrão de 19 polegadas, padrão EIA-310, ocupando no máximo 1U (44mm) do referido rack;
✓ Deverão ser fornecidos todos os cabos, suportes (se necessários, "gavetas", "braços" e "trilhos") para a instalação do equipamento no rack;
✓ Possuir painel frontal do tipo LCD com capacidade de apresentar informações a respeito da utilização de CPU, memória e tráfego de rede do equipamento;
✓ Dispor de fonte de alimentação com tensão de entrada de 110V a 220V AC (automática), e freqüência de 60Hz;
✓ Possuir painel/led indicativo de on/off do uso de disco e interfaces de rede;
✓ Possuir sistema operacional customizado especificamente para funções de UTM. Não serão aceitos sistemas de firewall que sejam executados sobre sistemas operacional em versões ou configurações distribuídas comumente no mercado, como o Novell NetWare, Microsoft Windows, Linux ou FreeBSD;
✓ Possuir um throughput mínimo de 1.000 (mil) Mbps para tráfego comum;
✓ Possuir um throughput mínimo de 530 (quinhentos e trinta) Mbps para tráfego criptografado (AES);
✓ Possuir no mínimo 4 (quatro) GB de memória RAM;
✓ Capacidade de estabelecer no mínimo 5.000 (cinco mil) túneis VPN simultaneamente;
✓ O equipamento deve suportar 4.000 (quatro mil) usuários logados simultaneamente para as regras de perfil de acesso;
✓ Suportar 800.000 (oitocentas mil) conexões simultâneas;
✓ As interfaces de rede deverão estar localizadas, na frente do equipamento;
✓ Possuir pelo menos 9 (Nove) interfaces de rede Gigabit Ethernet 10/100/1000 com leds indicativos de link e atividade;
✓ Possuir dispositivo de armazenamento interno de no mínimo 250 (duzentos e cinqüenta) GB;
✓ Possuir uma interface para configuração e gerenciamento através de interface de linha de comando CLI (Command Line Interface);
✓ O console do equipamento deverá ser acessado utilizando interface física específica para esta finalidade, do tipo serial DB-9, com conector RJ-45;
✓ O dispositivo deverá trabalhar com o conceito de refrigeração túnel de vento, possibilitando assim melhor refrigeração do dispositivo, desta forma prolongando sua vida útil;
✓ O fluxo de ar deverá obrigatoriamente ser: entrada de ar frio pela frente, saída de ar quente por trás do dispositivo;
✓ O sistema de coolers deverá ser do tipo gaveta removível, permitindo sua retirada ou inserção sem o uso de ferramentas;
✓ Possuir pelo menos 2 (duas) portas USB para inserção de dispositivos externos;
✓ No caso da porta(s) USB o equipamento deverá registrar as atividades de uso desta(s) porta(s), registrando informações, tais como: usuário que ativou ou desativou a porta, data e hora de ativação, etc.;
✓ Possuir manual de ajuda e interface em português;

5.20 - Servidor de Appliance Gerenciamento de Logs

✓ Deverá ser uma solução de software appliance e deve executar as seguintes funcionalidades primárias: coletar, comprimir, centralizar, agregar, normalizar, correlacionar e armazenar os logs (eventos) de diversos tipos de ativos e ferramentas computacionais. Dentro destas funcionalidades,

Folha Nº 286

encontram-se as capacidades de geração de alertas, definição de criticidade e agrupamento de incidentes, além de atender de forma integral os requisitos abaixo.

✓ Modulo de Gerencia o Possuir integração com base de conhecimento sobre atividades anômalas na Internet (origens de ataques, protocolos, etc), obtida automaticamente do site do Fabricante, permitindo a correlação dinâmica dessas informações com os dados coletados na rede local;

✓ A atualização da base de conhecimento sobre atividades anômalas na Internet deverá possuir periodicidade mínima diária;

✓ Possuir regras de correlação pré-definidas para detectar ataques, exploração de vulnerabilidades, códigos maliciosos, abusos de usuários, dentre outros cenários;

✓ O processo de correlação de eventos deve levar em consideração a normalização e base de conhecimento do fabricante, envolvendo efeitos, recursos e mecanismos utilizados;

✓ Possuir uma base de conhecimento contendo informações sobre vulnerabilidades e sugestões de remediação, apresentando os artigos relevantes ao incidente que está sendo analisado;

✓ Permitir a criação de tickets de resolução de incidentes. Possibilidade de incluir no Ticket os artigos da base de conhecimento relevantes ao incidente, e também permitir a inserção de tarefas adicionais manualmente;

✓ Fabricante da solução deve possuir laboratórios de pesquisa próprios, com visão global para detecção de novas ameaças e vulnerabilidades, para fornecer atualizações automáticas diárias para correlação dos eventos locais coletados;

✓ Console deve possuir indicador visual do nível de risco de segurança global de 1 a 4 (menos grave a mais grave), indicar a vulnerabilidade mais explorada mundialmente, eventos globais mais comuns em firewalls e ids mundiais;

✓ A solução deve conectar-se automaticamente ao fabricante múltiplas vezes ao dia para obter atualizações de assinaturas para associação automática de incidentes às respectivas vulnerabilidades;

✓ Deve fazer download automático de lista de IPs maliciosos e IPs de BotNet que foram detectados recentemente na Internet pelo fabricante da solução, e utilizar esta informação como parte da correlação de eventos;

✓ Ao detectar incidentes que contém tráfego originado por IPs das listas obtidas no fabricante, deve informar mais detalhes sobre como desde quanto este IP está listado, informações da rede a que o IP pertence (como provedor, pais), para auxiliar na investigação;

✓ Deve ter a capacidade de estabelecer métricas de desempenho sob atividades e processos críticos, disparando alertas na ocorrência de problemas potenciais;

✓ Deve ter a capacidade de investigar a causa raiz dos problemas, possibilitando explorar as informações pertinentes que são coletadas a partir de perspectivas múltiplas e em vários níveis de detalhamento;

✓ Deve fornecer um conjunto de serviços de integração via API – Application Programming Interface, para no mínimo os seguintes serviços abaixo:

✓ Gestão de ativos;

✓ Gestão de Permissões (sistema de arquivos);

✓ Gestão de Exceções;

✓ Gestão de Fontes de Evidências Estendidas;

✓ Gestão de Tarefas;

✓ Gestão de Padrões/Normas;

✓ Gestão de Papéis/Funções;

Comissão de Licitação
Folha Nº
287

✓ Deve ter a capacidade de executar coletas de dados de forma incremental, possibilitando ainda restringir o período de coleta dos eventos mais antigos;

✓ Deve ter a capacidade de importar individualmente ativos para a verificação, possibilitando categorizar por qual tipo de ativo será importado;

✓ Deve ter a capacidade de criar uma regra pré-definida e torná-la uma regra padrão para importação de ativos;

✓ Deve ter a capacidade de personalizar ativos em um ambiente de teste (laboratório) e importar no ambiente de produção, não necessitando repetir os passos para recriar o tipo de ativo desejado;

✓ Ter a capacidade de carregar e instalar a console de administração em um computador remoto;

✓ Modulo Análise de Vulnerabilidades

✓ Deve possuir um "engine" de varredura de vulnerabilidades de alto desempenho, em plataforma 64 bits;

✓ Deve permitir o gerenciamento dos scanners a partir de uma console única centralizada

✓ Deve possuir Controle de acesso a console baseado em papeis (RBAC – rolebased access control), usuários e funções;

✓ Deve incluir mecanismos para varredura de hosts, bancos de dados e aplicações web, incluindo a detecção de vulnerabilidades em AJAX e Web 2.0;
✓ Deve oferecer a varredura "segura" de sistemas SCADA – Supervisory Control And Data Acquisition;
✓ Deve ser capaz de avaliar mais de 54.000 testes de vulnerabilidades sobre mais de 14.000 vulnerabilidades;
✓ Deve ter a capacidade de atualizar automaticamente a tabela de ativos do Gerenciador de Incidentes Eventos e Segurança, preenchendo informações sobre os serviços e as vulnerabilidades encontradas no(s) ativo(s) analisado(s);
✓ Deve ter a capacidade de se atualizar dinamicamente a partir do site do fabricante, possibilitando a descoberta das vulnerabilidades mais recentes;
✓ Deve ter a capacidade de correlacionar os eventos baseados nos sistema operacional, Porta Protocolo, Banners e Vulnerabilidades;
✓ Deve ter a capacidade de detectar vulnerabilidades em aplicações baseadas em Web, bases de dados, aplicações comerciais, sistemas operacionais e dispositivos de rede;
✓ Deve ter a capacidade de gerar relatórios e varreduras pré-configurados para serem executados imediatamente ou agendados de forma diária, semanal e mensal;
✓ Capacidade de verificações de vulnerabilidades: de uma forma não invasiva, invasiva, por tipo de risco, categoria e CVE;
✓ Deve ter a capacidade de verificação de vulnerabilidades em ambiente Windows deve incluir: detecção de hot fixes, service packs, registros, backdoors, trojans, peer to peer e Antivirus;
✓ As vulnerabilidades devem ser categorizadas em Alto, Médio, Baixo e Informativo;
✓ Modulo Análise de Conformidades (Políticas, Frameworks e Normas)
✓ Deve oferecer um ambiente centralizado para a coleta e a gestão das evidências de conformidade com Políticas, Frameworks e Normas;
✓ Deve permitir o mapeamento de controles às políticas;
✓ Deve controlar o processo, workflow de edição, revisão, aprovação e aceitação (com ou sem exceção) das políticas;
✓ Deve controlar os prazos de cada etapa;
✓ Deve controlar as datas de revisão das políticas;
✓ Deve permitir a criação de dashboards dinamicos, acessíveis pela web, com suporte a "drill down" nas evidências;
✓ Deve oferecer uma API via Web Services para permitir a integração com processos externos, workflow e ticketing;
✓ Deve suportar de forma nativa os padrões da indústria, incluindo PCI, SOX, Cobit, ISO 27002, FISMA, HIPAA, GLBA, Basel II, CIS , NSA, dentre outros;
✓ Deve permitir a criação de um novo padrão técnico através da cópia de um padrão técnico pré-definido, permitindo alteração das checagens pré-definidas;
✓ Deve efetuar a desduplicação dos controles entre as várias políticas configuradas;
✓ Deve ser capaz de realizar a verificação de conformidade com determinada política, framework e norma, cobrindo tanto os requisitos técnicos (configurações dos ativos), quanto procedurais (conscientização dos usuários),
✓ de forma automatizada;
✓ Deve possuir console de administração de políticas integrado ao módulo de avaliação de controles técnicos, compartilhando a mesma infra-estrutura de console, servidor e base de dados;
✓ Deve possuir um repositório de políticas com workflow de edição, permitindo trabalhar a política através de fases com níveis de acesso diferenciado (ex: Rascunho, Em Revisão, Revisada, Aprovada, Publicada);
✓ Deve permitir ao usuário clicar numa opção que registre sua aceitação a política, rejeição, e também registrar dúvidas e solicitar exceção a política;
✓ Deve permitir a coleta automatizada de evidências de controles técnicos e procedurais;
✓ Possui módulo centralizador para a coleta e gestão das evidências de conformidade com políticas, frameworks e normas;
✓ Permite o controle de exceções às políticas, frameworks e normas, quando a aplicação da configuração recomendada gera impacto no ambiente, não podendo ser efetuada;
✓ Permite a integração com sistemas de service desk, para o encaminhamento de tickets de serviço para a correção das não conformidades;
✓ Suporta os sistemas operacionais Windows, UNIX e VMWare, bem como os servidores de aplicação IIS e Apache, através de bases de conhecimento/melhores práticas publicadas pelo SANS, NIST e CIS;
✓ Possui base de ativos, onde são armazenadas as informações pertinentes ao ativo, como:
✓ Características básicas do ativo (sistema operacional, versão de service pack);

Comissão de Licitação
Folha Nº
288

- ✓ Dono do ativo;
- ✓ Vulnerabilidades presentes no ativo;
- ✓ Resultado de análise de conformidade feitas sobre o ativo;
- ✓ Indicadores de Confidencialidade, Integridade e Disponibilidade;
- ✓ Rótulos para qualificar o ativo quanto à grupo, atividade, localidade, papel;
- ✓ Exceções às políticas, frameworks e normas à que o ativo está sujeito.
- ✓ Controles Técnicos:
- ✓ Deve trabalhar de forma nativa com a análise de conformidade de padrões técnicos, coletando informações do ambiente desejado e armazenando em sua base de dados;
- ✓ Deve executar as auditorias do ambiente utilizando os dados coletados e registrados na base de dados;
- ✓ Deve suportar a verificação de configurações e permissões nas plataformas Windows, Unix, Linux, Netware NDS, Oracle, SQL eExchange;
- ✓ A solução deve possuir uma base de dados de credenciais, onde serão armazenadas as senhas de acesso com privilégio aos diversos sistemas para uso nas auditorias automatizadas, não requerendo assim que o operador da solução tenha permissão nas máquinas alvo, e evitando digitação de credenciais a cada execução de auditoria;
- ✓ Deve suportar as melhores práticas de configuração definidas pelo NIS, SANS e/ou CIS para as seguintes plataformas:
- ✓ HP-UX;
- ✓ Solaris;
- ✓ VMWare ESX Server;
- ✓ AIX;
- ✓ Red Hat Enterprise Linux;
- ✓ SuSE Enterprise Linux;
- ✓ Windows XP;
- ✓ Windows Vista;
- ✓ Windows 7;
- ✓ Windows Server 2000;
- ✓ Windows Server 2003;
- ✓ Windows Server 2008;
- ✓ Deve possuir um mecanismo de gerenciamento de ativos, categorizadospor tipo, e baseado em um schema que possa ser expandido para suportar ativos que não estejam disponíveis out-of-the-box;
- ✓ Deve ser possível classificar os ativos quanto à Confidencialidade, Integridade e Disponibilidade (CIA);
- ✓ Deve ser possível associar os ativos à funções, processos ou papéis específicos;
- ✓ Deve utilizar as informações de CIA do ativo para pontuar o risco doativo;
- ✓ Deve permitir o gerenciamento de baselines de configuração dos ativos, que podem ser comparados com as novas avaliações para a determinação de desvios;
- ✓ Deve permitir o gerenciamento de permissões em arquivos, através de workflow de coleta/revisão/aprovação;
- ✓ Deve ter compatibilidade com o protocolo SCAP (Security Content Automation Protocol);
- ✓ Deve permitir a importação de evidências de conformidade de fontes externas, por CSV ou ODBC;
- ✓ Controles Procedurais:
- ✓ Deve permitir a criação de um novo padrão procedural através da cópia de um padrão procedural pré-definido, permitindo alteração das perguntas e respostas pré-definidas;
- ✓ Deve possuir um módulo de criação e publicação de questionários para usuários e análise de resultados, via web;
- ✓ Deve permitir determinar peso para cada pergunta e nível de risco para cada resposta;
- ✓ Deve permitir cascateamento de perguntas, de acordo com a resposta escolhida (ex: se respondeu "A" pule para pergunta "X", se respondeu "B" pule para pergunta seguinte);
- ✓ Deve permitir publicar os questionários via web, enviando um e-mail de convite para os usuários alvo, acessando o questionário e respondendo pelo seu navegador de internet;
- ✓ Deve possuir visualização gráfica do resultado do questionário, indicando por código de cores qual o risco computado de cada seção e perguntas;
- ✓ Deve possuir console de administração de políticas integrado ao módulo de avaliação de controles técnicos, compartilhando a mesma infra-estrutura de console, servidor e base de dados;
- ✓ Deve possuir um workflow de gerenciamento de políticas escritas, desde a edição a publicação para usuários;

✓ Deve possuir um repositório de políticas com workflow de edição, permitindo trabalhar a política através de fases com níveis de acesso diferenciado (ex: Rascunho, Em Revisão, Revisada, Aprovada, Publicada);
✓ Deve permitir ao usuário clicar numa opção que registre sua aceitação a política, rejeição, e também registrar dúvidas e solicitar exceção a política;
✓ Módulo de Monitoração Anti-Fraude
✓ Deve ter a capacidade de trabalhar em três camadas de autenticação, sendo no mínimo:
✓ Camada 1: Certificado SSL com Validação Extendida (Extended Validation Certificate);
✓ Camada 2: Autenticação do usuário por certificado digital padrão X-509 v.3 ou solução de OTP (One-Time Password);
✓ Camada 3: Autenticação Baseada em Risco e Detecção de Fraudes PorComportamento;
✓ Deve ter a capacidade de utilizar a autenticação baseada em risco em tempo real, categorizando o nível de risco de cada operação, evitando a fraude antes que ela ocorra;
✓ Deve ter a capacidade de aprendizado automático, balanceamento de peso dos parâmetros por usuário e capacidade de eliminar comportamentos obsoletos através de uma janela de tempo móvel e ajustável;
✓ Deve ter a capacidade de implementar séries temporais que identificam anomalias na frequência e distribuição temporal das transações do usuário
✓ Deve ter a capacidade de utilizar as listas estáticas e dinâmicas para vigiar origens suspeitas de transações, sendo no mínimo, números de , endereços IP e podem ser consultadas e atualizadas pelas políticas de análise
✓ de risco;
✓ Deve ter a capacidade de utilizar a pontuação de risco calculada pelos mecanismos de regras e comportamento, para implementar autenticações adicionais quando uma transação representar um alto risco de fraude;
✓ Deve ter a capacidade de ser implementado de forma não instrusiva, ou seja, sem a utilização de agentes e utilizar as informações enviadas dos atuais aplicativos de segurança como mais um parâmetro na categorização do nível de
✓ risco da operação;
✓ Deve trabalhar como um correlacionador comportamental, onde parâmetros comportamentais, em conjunto com regras pré-estabelecidas são utilizadas na análise;
✓ Deve ter a capacidade de identificar transações anomalas mesmo que não sejam categorizadas previamente como fraudes e autenticas;
✓ Deve ter a capacidade de gerar uma pontuação no nível de risco e iniciar uma tarefa previamente estabelecida;
✓ Deve ter a capacidade de correlacionar qualquer tipo de parâmetros, de forma ilimitada, com no mínimo, os parâmetros abaixo, atribuindo "pesos" diferenciados para cada parâmetro, conforme cada perfil de usuário e grupos analisados;
✓ Endereçamento IP;
✓ Localização Geográfica;
✓ Versão de sistema operacional de acesso;
✓ Browser utilizado no acesso;
✓ Idioma do sistema operacional e browser utilizado;
✓ Dados de data e hora das operações cotidianas;
✓ Valor médio da operação realizada;
✓ Dados de frequência (Data/Hora/Dia da Semana/Dia do Mês);
✓ Tipo e Categoria de usuário;
✓ Tipo e Categoria de operação de movimentação Financeira;
✓ Capacidade de validar uma ação como autentica e fraude, através do cruzamento das informação obtidas com as ações lógicas (operações de Login) e geográficas (localização de execução das ações lógicas);
✓ Capacidade de importar logs comportamentais de ferramentas de terceiro;
✓ A solução deve possuir módulos de atuação multi-canal, com no mínimo:
✓ Internet Banking (Login e Movimentações Financeiras);
✓ ATM;
✓ Phone-Banking;
✓ Mobile Banking;
✓ Deve ter a capacidade de executar no mínimo 1.500 transações por segundo, sem a ocorrência de degradação de performance na experiência do usuário;

5.21 - Servidor de Appliance de Segurança de e-Mail

Comissão de Licitação
Folha Nº
290

✓ O equipamento deve se instalar em rack com largura padrão de 19 polegadas, padrão EIA-310, ocupando no máximo 1U (44mm) do referido rack;
✓ Deverão ser fornecidos todos os cabos, suportes (se necessários, "gavetas", "braços" e "trilhos") para a instalação do equipamento no rack;
✓ Possuir painel frontal do tipo LCD com capacidade de apresentar informações a respeito da utilização de CPU, memória e tráfego de rede do equipamento;
✓ Dispor de fonte de alimentação com tensão de entrada de 110V a 220V AC (automática), e freqüência de 60Hz;
✓ Possuir painel/led indicativo de on/off do uso de disco e interfaces de rede;
✓ Possuir sistema operacional customizado especificamente para funções de UTM.Não serão aceitos sistemas de firewall que sejam executados sobre sistemas operacional em versões ou configurações distribuídas comumente no mercado, como o Novell NetWare, Microsoft Windows, Linux ou FreeBSD;
✓ Capacidade de tratamento de 8.000 (oito mil) e-mails/hora;
✓ Possuir no mínimo 2 (dois) gigabytes de memória RAM;
✓ Possuir no mínimo 3 (três) interfaces de rede 10/100/1000 RJ45;
✓ Possuir dispositivo de armazenamento interno de no mínimo 80 (oitenta) GB;
✓ Possuir uma interface serial (padrão DB-9 ou semelhante), para configuração e gerenciamento através de interface de linha de comando CLI (Command LineInterface);
✓ Possuir pelo menos 2 (duas) porta USB para inserção de dispositivos externos;
✓ Possuir manual de usuário completo, interface de administração, ajuda on-line e demais documentos correlatos em português;
✓ Implementar os protocolos SMTP/ESMTP seguindo especificações da RFC2821, RFC 2822 e RFC 2554;
✓ Possibilitar a intermediação transparente, para o usuário, do processo de negociação de mensagens eletrônicas no papel de gateway SMTP ou de MTA, podendo efetuar diversos tipos de modificações nas mesmas;
✓ Possuir interface de administração gráfica para o usuário do tipo WEB sobre SSL;
✓ Possuir interface gráfica nativa, remota, com tráfego cifrado para as plataformas Linux e Windows. Ela deve permitir gerenciar mais de um gateway ao mesmo tempo;
✓ Possibilitar filtragens de mensagens eletrônicas para atuar no combate a vírus epara controle de tipos de anexos, tamanhos de anexos, palavras-chave, expressões regulares, endereços eletrônicos de remetentes e destinatários, remetentes, servidores, RBLs (configuráveis), URLs;
✓ Implementar autenticação ESMTP dos tipos PLAIN e LOGIN;
✓ Possuir sistema de controle de relay por domínios, redes, endereços IP e autenticação ESMTP;
✓ Implementar filtragem de antivírus, interna e integrada ao sistema, que permita atualização de novas vacinas e assinaturas de forma automática;
✓ Possuir um sistema de confirmação de mensagens que vise proteger o(s) domínio(s) gerenciados pelo produto contra mensagens de SPAM com as seguintes características:
✓ Deve possibilitar a configuração da filtragem de maneira global (para todos os usuários da rede) ou particular. Nesta última opção, deve permitir que cada usuário configure parâmetros como listas de endereços autorizados e não autorizados e inclusive opte por não utilizar o sistema de confirmação se assim desejar, através de uma interface WEB compatível com Internet Explorer e Mozilla Firefox;
✓ Deve possibilitar proteção anti-bot no mecanismo de confirmação de mensagens;
✓ Suportar a criação de clusters com tolerância a falhas;
✓ Permitir bloqueio da conexão ao gateway seguro de e-mail caso o IP de origem da conexão não possua registro de DNS reverso válido publicado na Internet;
✓ Permitir a exportação de logs e/ou eventos por e-mail ou FTP;
✓ Permitir que a ordem de aplicação dos filtros internos seja alterada;
✓ Permitir uso de listas bloqueio ou aceite de remetentes e/ou domínios de forma global ou geral, por grupo de usuários ou por usuários;
✓ Registrar em log todo e-mail mal formatado ou que não siga completamente a RFC de referencia para o protocolo do SMTP e permitir que o administrador da ferramenta escolha se o e-mail deve ser encaminhado para o servidor de destino ou se ele deve ser salvo para avaliação posterior;
✓ Permitir notificação automática de uso da quarentena para o administrador, para o usuário ou para ambos;
✓ A interface de gestão do repositório de quarentena do usuário deve permitir que listas de bloqueio e listas confiáveis sejam importadas e exportadas;
✓ A interface de gestão do repositório de quarentena do usuário deve permitir que as mensagens salvas sejam classificadas como confiáveis (não são SPAM) ou como não confiáveis (SPAM);
✓ Permitir filtragem de e-mails baseado em categorias de URLs;
✓ A atualização da base de URLs deve ser configurável pelo administrador;

Folha Nº 093

✓ Filtro de detecção de SPAM bayesiano interno, integrado ao appliance, com as seguintes características:
✓ Fornecimento de todas as atualizações de software assim como a atualização da base de conhecimento (novas regras de detecção de SPAM), pelo período do contrato;
✓ Deverá avaliar as mensagens e atribuir uma nota a cada uma delas, que corresponda à probabilidade da mesma ser SPAM, variando de 0 a 100%;
✓ As notas atribuídas às mensagens deverão ser calculadas utilizando-se bancos de dados com informações estatísticas obtidas de milhares de mensagens de email, e produzidas através de análise bayesiana;
✓ Os bancos de dados com informações estatísticas deverão poder ser atualizados diária e automaticamente, através de download via Internet;
✓ Deverá possuir dois modos distintos de atribuição de notas para as mensagens: um que prioriza a detecção de SPAM e outro que reduz os falso-positivos;
✓ Deverá possibilitar que os usuários realizem treinamento do banco de dados de mensagens informando, para cada mensagem recebida, se a mesma é ou não SPAM;
✓ Permitir a criação de bases de dados de classificação distintas para cada usuário ou grupo de usuários, a fim de que cada base represente um perfil de usuário ou grupo de usuários específicos;
✓ Permitir mecanismo que faça com que o treinamento de cada usuário seja aproveitado somente na base correspondente a seu grupo ou usuário do sistema;
✓ Permitir o backup e restauração das bases com os treinamentos dos usuários via interface de administração remota;
✓ Deverá possuir plugins para realização do treinamento das mensagens pelo menos para os clientes de e-mail Microsoft Outlook e Thunderbird;
✓ Deverá possuir mecanismo de treinamento de mensagens para os leitores de email para os quais não exista plugin disponível, através da modificação da mensagem original. Esta modificação deverá funcionar para qualquer cliente de e-mail que suporte a leitura de mensagens HTML;
✓ Possibilitar o registro de todas as classificações e treinamentos realizados através do servidor, e de todas as tentativas de abertura de sessões ou conexões que forem recusadas pelo mesmo;
✓ Possibilitar o registro de todas as operações envolvendo as bases de dados do sistema de detecção, tais como download, upload e recálculo;
✓ Possibilitar registro da remoção, restauração ou criação de backup de bases;
✓ Possuir mecanismo que permita a configuração do log (tempo de permanência das mensagens, tamanho de arquivo, etc) e visualização das mensagens de log através da interface gráfica;
✓ Possibilitar o envio de registros para o sistema operacional (syslog no caso de sistemas UNIX e Event Viewer em Windows);
✓ Possuir manual de ajuda e interface em português;

5.22 - No-break 2Kva e Acessórios

✓ Capacidade de 2 KVA
✓ Autonomia mínima de 160 minutos com carga plena
✓ Forma de onda Senoidal na saída
✓ Tensão de entrada de nominal de 120 volts
✓ Freqüência autosensing de 40 a 70 Hz
✓ Quatro tomadas de saída no padrão NEMA (5-15R)
✓ Gabinete de 2U de montável no formato torre ou rack
✓ Baterias internas
✓ Conexão para baterias externas para aumento de autonomia
✓ Capacidade de by-pass automático e manual
✓ Leds indicadores de ligado, by-pass, bateria e entrada AC
✓ Leds indicadores de carga da bateria
✓ Desenho "True On Line" com tempo zero de transferência
✓ Supressor de transientes e surtos integrado
✓ Capacidade de conversão de freqüência
✓ Software de gerenciamento com as funções
✓ Seleção da tensão de saída entre os valores 100, 110, 115, 120, 127V
✓ Habilitar ou desabilitar auto restart
✓ Habilitar ou desabilitar a detecção de reversão de neutro
✓ Selecionar modo de conversão de freqüência
✓ Alterar o aviso de bateria fraca do padrão de 2 minutos
✓ Selecionar quantidade de testes de bateria
✓ Desabilitar teste de bateria automático

Comissão de Licitação
Folha Nº
29.2

✓ Programar a autonomia do no-break de acordo com o numero de baterias conectadas (externas)
✓ Interface de comunicação para controlar e monitorar o no-break compatível com SNMP e gerenciamento Web
✓ Imunidade a surtos de acordo com a norma IEEE 587 Categoria A & B
✓ Garantia mínima de 1 ano
✓ Nobreak de 2Kva para a sua melhor automação deverá ser acoplado os seguintes acessórios:
✓ Bateria Automotiva de 45 A;
✓ Terminal de Bateria 45 A Blindado.

5.23 - CABOS ELÉTRICOS 1kV, 2x2,5mm2

✓ Condutor: Cobre eletrolítico nu, encordoamento classe 5, NBR NM 280;
✓ Isolação: Composto termoplástico de PVC sem chumbo;
✓ Enchimento: PVC sem chumbo;
✓ Suas características atendem aos requisitos da NBR 7288;
✓ Cobertura: Composto termoplástico de PVC, com características de não propagação de chama;
✓ Isolamento elétrico: 1kV;
✓ Bitola: 2x2,5 mm2.

5.24 - NOBREAK 600VA

✓ Deverá ser microprocessado;
✓ Deve suportar no mínimo 600VA;
✓ Deve possuir potência de pico nominal de 300W;
✓ Deve possuir forma de onda semi-senoidal;
✓ Deve possuir auto teste para verificação das condições iniciais do equipamento;
✓ Deve permitir ligá-lo mesmo na ausência de rede elétrica;
✓ Deve permitir recarga automática da bateria mesmo com o nobreak desligado;
✓ Possuir gabinete metálico com pintura epóxi;
✓ Possuir gabinete anti-chama;
✓ Deve possuir bateria selada e a prova de vazamento;
✓ Deverá atender a norma NBR 14136 para tomadas de entrada e saída;
✓ Deverá possuir entrada bivolt 120/220V automático com saída fixa 120V;
✓ Deverá possuir chave liga/desliga;
✓ Deverá possuir proteção contra surtos de tensão;
✓ Proteção contra sub e sobretensão na rede elétrica com retorno e desligamento automático;
✓ Possuir proteção contra descarga profunda de bateria;
✓ Deverá possuir proteção contra sobrecarga e curto-circuito no inversor;
✓ Gerenciamento de bateria com aviso para substituição;
✓ Deve possuir peso líquido menor que 6 kg;
✓ Deve ser fornecido com garantia mínima de 02 (dois) anos;
✓ Deve possuir autonomia mínima de 30 minutos com carga completa.

5.25- SWITCH CENTRAL

✓ A solução poderá ser composta por equipamento modular (chassis) ou equipamentos empilháveis devendo, em qualquer um dos casos, atender todos os requisitos aqui especificados;
✓ A solução deverá ser montável em rack 19" devendo vir acompanhada dos acessórios necessários para tanto;
✓ Deve disponibilizar também Web Server interno com SSL, agente SNMPv1, v2 e v3;
✓ Deve permitir a criação de listas de controle de acesso (ACLs) complexas, com múltiplos parâmetros de comparação e ação, que permitem a modificação, encaminhamento, descarte ou priorização de pacotes;
✓ Deve possibilitar a construção de LAN's virtuais, no mínimo, 1.000 VLAN's definidas na norma IEEE 802.1Q simultaneamente, oferecendo ainda a funcionalidade de "doubletagging" (Q-in-Q), permitindo a criação de serviços TLS;
✓ O equipamento deverá possuir a quantidade e tipo de interfaces ópticas necessários e suficientes para ativação da topologia de rede óptica de atendimento às câmeras a serem instaladas, além de no mínimo 20 portas 1Gbit/s SFP e 2 portas RJ-45 10/100/1000 Mbps Ethernet fixas (em caso de conversores, os mesmo deverão ser fornecidos) ou em cartões SFP 1000Base-T instalados;
✓ Backplane passivo non-blocking, com suporte mínimo em Gbit/s para 70 imagens em resolução máxima das 70 câmeras de forma simultânea, mais 30% do valor total obtido para fins de expansão;
✓ Deve suportar roteamento estático e dinâmico.
✓ O equipamento deve possui interface de linha de comando com auxílio automático na sintaxe de comando e parâmetros, acessível através de SSH e/ou Telnet e/ou Console RS232;
✓ A solução deve suportar instalação de fonte de alimentação redundante

✓ No caso de solução com equipamentos empilháveis, deverão ser fornecidos o(s) modulo(s) e cabo(s) necessário(s) para empilhamento com outro equipamento da mesma família;
✓ No caso de solução modular, deverá ser fornecido com os módulos de supervisão e processamento necessários ao pleno atendimento dos demais requisitos dessa especificação;
✓ Deve ser possível limitar o número de endereços MAC aprendidos por cada porta.
✓ Deve implementar ajuste de data e hora do sistema utilizando NTP ou SNTP;
✓ Deve implementar mecanismo de supressão de Broadcast, permitindo a configuração por porta;
✓ Deve implementar mecanismo de controle de flood para tráfego broadcast, multicast e unicast;
✓ Deve implementar servidor web interno que possua interface de gerenciamento baseada em web (http ou https);
✓ Para implementação de QoS o equipamento deve possui no mínimo 04 (quatro) filas por porta, com algoritmos de priorização que permitem definir que determinado fluxo de dados sempre terá prioridade, configurar pesos para cada fila, definir taxas mínimas de encaminhamento;
✓ No caso de solução com equipamentos empilháveis, deverão ser atendidos os seguintes requisitos:
✓ O empilhamento deverá ser implementado em topologia de anel fechado, utilizando interconexões bidirecionais, de forma a manter o funcionamento da pilha mesmo em caso de falha em equipamentos individuais, cabos e conexões;
✓ A pilha deverá ser gerenciada através de um único endereço IP;
✓ Deve apresentar mecanismos que garantam segurança na operação e manutenção da planta instalada. Além da utilização de criptografia nos protocolos de comunicação, deve ser possível especificar através de filtros quais máquinas da rede podem acessar os equipamentos administrativamente;
✓ No caso de solução com equipamento modular, deverão ser atendidos os seguintes requisitos:
✓ Deve permitir empilhamento realizado por caminhos redundantes bidirecionais, de forma que a interrupção de uma conexão de stack ou desligamento de uma unidade não cause a ruptura do conjunto;

5.26 - Ponto Rede Lógica Cat6

✓ Os Pontos de rede logica são compostos por: Cabo de rede blindado de 8 vias categoria 6 e conector RJ45 categoria 6.
✓ O fornecimento e instalação do cabeamento da área de trabalho compreende todos os passos necessários para instalação dos cabos de rede, conectores, tomadas lógicas e certificação, manobras e identificações, de forma a tornar o ponto de rede do usuário funcional, incluindo as seguintes atividades e materiais
✓ Lançamento de 30 metros (média) de cabo UTP 24 AWG 4 pares, categoria 6;
✓ Quando a instalação for feita a partir do rack principal, o tamanho médio do cabo
✓ UTP deverá ser de 60 metros;
✓ Realização de conexões em patch panel ou bloco 110;
✓ Realização de conexões em tomada lógica RJ45;
✓ Efetuar testes e certificações;
✓ Ativação do ponto de rede nos switches, quando este tiver porta disponível. Ativar pontos de rede na estação do usuário
✓ Elaborar o "as built".
✓ Fornecimento e instalação 1 metro linear de infra-estrutura de acesso, compreende todos os passos necessários para disponibilizar a passagem adequada de cabos dos pontos de consolidação ou mutuo à estação de trabalho dos usuários, incluindo as seguintes atividades e materiais:
✓ Canaletas ou tubulação
✓ Curvas
✓ Materiais de acabamento
✓ Parafusos com bucha, abraçadeiras
✓ Fazer furos para fixar calhas ou tubos
✓ Recortar calhas ou tubos
✓ Fazer fixação

5.27 - Caixas Herméticas

✓ As Caixas Herméticas servirão para proteger os equipamentos do clima e do tempo com as seguintes especificações:
✓ Caixa Hermética com Grampo U e 2 prensa cabos - Cor Cinza, PP com proteção UV e estabilizador térmico, Sistema de trava, Travamento manual Flip Top, Sistema de proteção contra violação, Local para colocação de lacre, Sistema de vedação Anel de borracha - tipo o'ring, Tamanho 248 x 298 x 105 mm.

Comissão de Licitação
Folha Nº
296

✓ Caixa Hermética de Aço com Fechadura - Cor Cinza, Top, Sistema de proteção contra violação, Sistema de vedação, Anel de borracha - tipo o´ring, Tamanho 600mm x 500mm x 200 mm.
✓ Caixa Hermética de Aço com Fechadura - Cor Cinza, Top, Sistema de proteção contra violação, Sistema de vedação, Anel de borracha - tipo o´ring, Tamanho 40 x 30 x 20 Centímetro.

5.28 - Kit Aterramento

Para realização dos serviços, a empresa deverá executar a cravação a percussão das hastes terra em local externo onde haja exposição à chuva.

✓ Deverá ser utilizado um mínimo de 3 (três) hastes de 1,5m, preferencialmente colocadas em triângulo, de forma a deixar o valor de resistência menor que 2 Ohms e o valor de tensão entre neutro e terra menor que 1V. A fixação do condutor na haste deverá ser feita através de conector. A malha de aterramento (hastes e os condutores) deverá estar aterrada em uma profundidade de 20cm, sendo colocado um cap de PVC em cada haste para proteção dos conectores. As proteções de caps deverão ser fornecidas pela CONTRATADA. Os condutores para ligação a terra serão tão curtos e retilíneos quanto possível, sem emendas e protegidos contra corrosão, cortes ou danos. Deverá ser colocada um caixa de inspeção para aterramento, a ser fornecida pela CONTRATADA.
✓ O aterramento deverá ser interligado ao quadro de disjuntores mais próximo por cabo de 16mm2. Não serão de responsabilidade da CONTRATADA as obras civis para execução do serviço.

5.29 - Acessórios Secundários da Estrutura de Dados, , Imagem e Aplicativo

✓ Suporte para Fixação das antenas feito em cano galvanizado de 1 polegada com os acessórios necessários para a sua fixação,
✓ Eletroduto Flexivel reforçado de 1 polegada antichama,
✓ Abraçadeira de Nylon 7,6mm x 200mm, com proteão UVB
✓ Adesivo de Silicone incolor 280G,
✓ Fita Isolante PVC 19mm x 10mm,
✓ Cabo de Energia PP flexível trifasio 3 x 4 mm,
✓ Fita Isolante Auto Fusao 19mm x 2m,
✓ Tomada Padrao 2 pinos T com aterramento 20 A linha externa,
✓ Cabo de Cobre Flexivel 6mm 750v,
✓ Tomada de Filtro com proteção com contador de surtos elétricos com 8 tomadas transparente,
✓ Kit Cliente Acessórios I (Fita de Alumínio para fixação no Poste, FE),
✓ Mastro Galvanizado ¾ bitota de 2mm, vara com 3 metros,
✓ Kit Cliente Acessórios II Praças (Base, arame galvanizado, luvas, canos, canaletas 20mm x10mm).
✓ Encabeçamento Completo (1 Bap 3, 1J, 2 SIPA, 2 alça pré-formada de 6mm, arame de espinar)
✓ Passagem Completa (1 Bap 3, 1J, 1 SIPA e arame de espinar)

Comissão de Licitação
Folha Nº
295

6. Considerações Gerais para todos os itens

Prazo para instalação e configuração de toda a Rede de Dados, e Imagem será de até 40 (quarenta) dias, contados após recebimento da ordem de serviço pela empresa.

Deverão ser fornecidos catálogos originais ou proveniente da Internet, manual de instruções e serviços em língua portuguesa ou inglesa com marca e modelos fornecidos pelos fabricantes dos produtos ofertados, de acordo com as especificações mínimas exigidas para cada item.

Deverão ser fornecidos todos os dispositivos e acessórios necessários para a montagem e ao funcionamento dos produtos ofertados.

Os equipamentos fornecidos e instalados para o contratante deverão ser em regime de comodato.

Antes de iniciar a instalação de toda estrutura a Contratada deverá entregar no Almoxarifado Central, local, de segunda à sexta-feira, das 8:00 ás 12:00 e das 14:00 às 17:00 horas, (horário de Brasília-DF), ou onde a Administração necessariamente indicar, que terá o prazo de até 05 (cinco) dias para aceitar o mesmo, emitindo um documento de aceite, para somente após o licitante poderá começar a execução dos serviços.

7. Atividades a Serem Realizadas

A Contratada deverá projetar, entregar, instalar e montar os equipamentos objeto deste fornecimento de acordo com as quantidades a serem determinadas pela contratante.

8 Elaboração do Projeto Executivo

A empresa contratada deverá preparar o Projeto Executivo do Projeto de implantação da Rede de Dados , Imagem e Aplicativo que deverá ser aprovado previamente pela Prefeitura Municipal de Pindoretama antes da execução da obra. O projeto deverá ser realizado conforme as normas estabelecidas no Termo de Referência.

O Projeto Executivo deverá ser aprovado pela Prefeitura Municipal de Pindoretama. Obrigatoriamente o projeto deverá utilizar a solução proposta, apresentada na fase da licitação. Qualquer necessidade em alterar as normas estabelecidas em função de impossibilidades encontrada na etapa de levantamento, a mesma deverá ser aprovada pela Prefeitura Municipal de Pindoretama.

O Projeto Executivo deverá conter plantas detalhadas produzidas em sistema CAD, que serão entregues em arquivo formato DWG (Autocad – R14) ou DXF, relatórios e memoriais descritivos serão entregues em Microsoft Word ou OpenOffice Write e Planilhas em Microsoft Excel ou OpenOffice Calc. A empresa contratada deverá entregar os projetos da seguinte maneira:
2 (duas) cópias em meio digital (CD ou DVD);
2 (duas) cópias em papel.

9. Fases de Implementação e Prazos

O prazo de garantia dos equipamentos não poderá ser inferior a 01(um) ano, contados da instalação do mesmo.
A contratada deverá disponibilizar local ou (0800) para que os servidores autorizados pela Prefeitura de Pindoretama possam realizar abertura de chamados técnicos. Adicionalmente, a contratada poderá disponibilizar e-mail ou sítio na Internet para abertura de chamados de suporte técnico. O disponibilizado da contratada deverá permanecer disponível para abertura de chamados técnicos 24 horas por dia, 7 dias por semana, durante todo o período de vigência da Contrato;

Modalidades de Suporte Técnico:

O prazo de atendimento para prestação do serviço de suporte técnico na modalidade manutenção de atendimento telefônico é de até 02 (duas) horas;
O prazo de reparação para prestação do serviço de suporte técnico na modalidade manutenção corretiva é de até 48 (quarenta e oito) horas;
Define-se prazo de reparação como o tempo decorrido entre a abertura do chamado técnico, efetuado pelo técnico autorizado pela prefeitura de Pindoretama à futura contratada e a efetiva recolocação do equipamento em seu estado normal de funcionamento, descontado o tempo de deslocamento do técnico de seu local de origem até a Prefeitura.
Admite-se a substituição temporária do equipamento ou componente com defeito por outro de mesmas características técnicas.

Relatório Mensal de Chamados Técnicos

Todos os chamados técnicos abertos devem ser obrigatoriamente registrados pela contratada para que haja um acompanhamento do serviço de suporte técnico.
A contratada deverá disponibilizar para a Prefeitura de Pindoretama, até o 5° (quinto) dia do mês subsequente, relatório mensal, no formato HTML ou PDF, referente a todos os chamados abertos no mês anterior, contendo, no mínimo, as seguintes informações:
a) número do chamado;
b) número(s) de série do(s) equipamento(s) afetado(s);
c) defeito reportado;
d) solução provisória (se for o caso);
e) solução definitiva;

Comissão de Licitação
Folha Nº
2016

Equipamentos a serem fornecidos:

Todos os equipamentos e componentes fornecidos deverão ser novos e em estado de primeiro uso, não sendo aceitos produtos com fabricação descontinuada por seus fabricantes;

10 – Metodologia

A CONTRATADA deverá confeccionar um plano de instalação incluindo metodologia e cronograma de implantação da solução, definindo atividades, prazos, responsabilidades e recursos utilizados para a instalação, testes e simulações e migração;
O plano de instalação deverá ser entregue ao Gestor do Contrato na reunião de alinhamento;
O plano de instalação deverá ser entregue em documento(s) eletrônico(s) em formato Office ou .pdf, e impresso, em formato A4;
Todos os trabalhos de instalação efetuados deverão ser acompanhados pelo Gestor do Contrato e da equipe técnica da CONTRATANTE;
A CONTRATADA deverá se reportar, antes de qualquer ação e decisão, ao Gestor do contrato;
Todos os detalhes/procedimentos de instalação e configuração dos softwares adquiridos deverão ser documentados pela CONTRATADA e entregues à CONTRATANTE em documento(s) eletrônico(s) em formato Microsoft Word ou Open Office Write, e impresso, em formato A4;
O processo de instalação e configuração será realizado, integralmente pela CONTRATADA, de acordo com o plano de instalação, devendo ser acompanhado pela equipe técnica designada pela CONTRATANTE;
O projeto deverá ser conduzido segundo as melhores práticas e metodologias existentes para projetos de infraestrutura, tendo como gerente responsável pelo projeto um profissional da CONTRATADA com conhecimento em ITIL;

A Adjudicatária deverá substituir, arcando com as despesas decorrentes, os produtos que apresentarem defeitos e irregularidades ou qualquer característica discrepante às exigidas no Edital e seus Anexos, ainda que constatados depois do recebimento e/ou pagamento.

Comissão de Licitação
Folha Nº
097

Pindoretama/CE, 11 de dezembro de 2023.

Paulo Henrique Horácio Freires
Secretário de Administração.

Cristiano do Nascimento Alves
Gabinete do Prefeito/controlador adjunto.

Leonardo Mendes Oliveira
Ordenador de Despesas da Secretaria de Educação e Juventude.

Rosana Barbosa de Lima
Secretária do Turismo e Desenvolvimento Econômico.

Eli da Silva Costa
Secretário de Infraestrutura e Serviços Públicos.

JOSÉ ADERVAL DA SILVA
Secretário da Saúde.

Edinardo Miranda Cândido
Secretário do Meio ambiente Desenvolvimento Agropecuário.

Leonardo Hilário de França
Secretaria de Finanças

Francisco Costa Monteiro
Secretaria de Cultura

RONALDO LUIS DE ALMEIDA
Ordenador de Despesas da Secretária do Trabalho e Desenvolvimento Social.

José Marcelo Rocha Holanda
Secretário do Desporto e Lazer.

ANEXO II
MODELO DE PROPOSTA
(ESTE DOCUMENTO SOMENTE DEVERÁ SER APRESENTADO APÓS A FASE DE DISPUTA)

À
Comissão Permanente de Licitação
Prefeitura Municipal de Pindoretama/CE.

Ref.: Pregão Eletrônico nº __.__.__/____.

Pelo presente instrumento, vimos apresentar nossa proposta de preços relativa ao objeto desta licitação, bem como as informações, condições da proposta e declarações exigidas no Edital do pregão acima citado.

1. Identificação do Licitante:

- Razão Social:
- CNPJ e Inscrição Estadual:
- Endereço completo:
- Telefone, fax, e-mail:
- Banco, Agência e nº da conta corrente

2. Condições Gerais da Proposta:

- A presente proposta é válida por XX (xxxx) dias contados da data de sua apresentação.

3. Pelo presente, a empresa acima qualificada, por meio do signatário, que legalmente a representa, declara e garante que:

- Examinou cuidadosamente todo o Edital e Anexos e aceita todas as condições nele estipulados e que, ao assinar a presente declaração, renuncia ao direito de alegar discrepância de entendimento com relação ao Edital;
- Que cumpre plenamente as disposições normativas relativas ao trabalho do menor, contida na Lei nº 9.854, de 27/10/1999 e na Constituição Federal de 1988;
- Que tomou conhecimento de todas as informações e das condições para cumprimento das obrigações, objeto da presente licitação;
- Que sua proposta engloba todas as despesas referentes ao fornecimento, bem como todos os tributos, encargos sociais e trabalhistas, garantia, frete e quaisquer outras despesas que incidam ou venham incidir sobre o objeto da licitação.

Obs.: O proponente deverá declarar, sob as penalidades da lei, a existência de fato superveniente impeditivo de sua habilitação, somente se houver.

PROPOSTA DE PREÇOS:

ITEM	ESPECIFICAÇÕES	QUANT.	UNID.	VALOR UNIT.	VALOR GLOBAL

Discriminar, o valor individual de cada item conforme especificações e quantitativos constantes do Quadro I, do Anexo I do Edital.

(Local e data).

Nome e assinatura
Número do Documento de identidade
Número do C.P.F.
Cargo

OBS.: Esta Proposta deverá ser emitida preferencialmente em papel timbrado da empresa proponente e carimbada com o número do C.N.P.J.

ANEXO III
MODELO DE DECLARAÇÃO DE INEXISTÊNCIA DE FATOS IMPEDITIVOS

Edital nº _____

(Nome da empresa), inscrita no CNPJ sob n.º XX.XXX.XXX/XXXX-XX, sediada à (endereço completo), DECLARA sob as penas da Lei que até a presente data inexistem fatos impeditivos para sua habilitação no processo licitatório supracitado e, da mesma forma ainda estar ciente da obrigatoriedade em declarar ocorrências posteriores inerentes ao processo licitatório em questão.

(Local e data).

Nome e assinatura
Número do Documento de identidade
Número do C.P.F.
Cargo

OBS.: Esta declaração deverá ser emitida preferencialmente em papel timbrado da empresa proponente e carimbada com o número do C.N.P.J.

Comissão de Licitação
Folha Nº
301

ANEXO IV
MODELO DE DECLARAÇÃO DE CUMPRIMENTO DOS REQUISITOS DE HABILITAÇÃO

Edital nº _____

(Nome da empresa) inscrita no CNPJ sob n.º XX.XXX.XXX/XXXX-XX, sediada à (endereço completo), DECLARA sob as penas da lei que cumprem plenamente os requisitos de habilitação, sob pena de sujeição às penalidades previstas no Edital.

(Local e data).

Nome e assinatura
Número do Documento de identidade
Número do C.P.F.
Cargo

OBS.: Esta declaração deverá ser emitida preferencialmente em papel timbrado da empresa proponente e carimbada com o número do C.N.P.J.

Comissão de Licitação
Folha Nº
302

ANEXO V

MODELO DE DECLARAÇÃO DE MICROEMPRESA OU EMPRESA DE PEQUENO PORTE

Edital nº _____

(Nome da empresa) inscrita no CNPJ sob n.º XX.XXX.XXX/XXXX-XX, sediada à (endereço completo), DECLARA sob as penas da lei, sem prejuízo das sanções e multas previstas neste ato convocatório, que é Microempresa ou Empresa de Pequeno Porte, nos termos do enquadramento previsto na Lei Complementar nº 123, de 14 de dezembro de 2006, cujos termos declaro conhecer na íntegra, estando apta, portanto, a exercer o direito de preferência como critério de desempate no procedimento licitatório, realizado pelo Município de Pindoretama, Estado do Ceará.

(Local e data).

Nome e assinatura
Número do Documento de identidade
Número do C.P.F.
Cargo

OBS.: Esta declaração deverá ser emitida preferencialmente em papel timbrado da empresa proponente e carimbada com o número do C.N.P.J.

ANEXO VI
DECLARAÇÃO DE SITUAÇÃO REGULAR PERANTE O MINISTÉRIO DO TRABALHO

Edital nº _____

(Nome da empresa). Inscrita no CNPJ sob n.º XX.XXX.XXX/XXXX-XX, sediada à (endereço completo), DECLARA, sob as penas da lei, para fins de habilitação no Pregão Eletrônico ____/___, bem como para atendimento ao disposto no inc. V do art. 27 da Lei 8.666, de 21 de junho de 1993, acrescido pela lei 9.854, de 27 de outubro de 1999, que não emprega menor de dezoito anos em trabalho noturno, perigoso ou insalubre, bem como não emprega menor de dezesseis anos, salvo na condição de aprendiz

(Local e data).

Nome e assinatura
Número do Documento de identidade
Número do C.P.F.
Cargo

OBS.: Esta declaração deverá ser emitida preferencialmente em papel timbrado da empresa proponente e carimbada com o número do C.N.P.J.

Comissão de Licitação
Folha Nº

ANEXO VII
MINUTA DO CONTRATO

CONTRATO Nº _____

Contrato que entre si celebram de um lado o MUNICÍPIO DE PINDORETAMA/CE, por intermédio da Secretaria de _____ e a empresa _____, para o fim que nele de declara.

O MUNICÍPIO DE PINDORETAMA/CE, pessoa jurídica de direito público interno, com sede na Rua: Juvenal Gondim, nº 221. CEP: 62.860-000. Centro – Pindoretama, Estado do Ceará, inscrito no CNPJ sob o nº 23.563.448/0001-19, por intermédio da Secretaria Municipal de _____, doravante denominada **CONTRATANTE**, neste ato representado pelo (a) Secretário (a) Municipal de _____, Sr(a). _____, CPF nº _____ e a empresa _____, doravante designada **CONTRATADA**, inscrita no CNPJ/MF sob o nº _____, sediada na _____, nº ____. Bairro: _____. CEP: _____, telefone _____, em _____, Estado do _____, neste ato representada pelo(a) Sr.(a). _____ portador da Cédula de Identidade nº _____ expedida pela(o) _____ e CPF nº _____, resolvem celebrar o presente Termo de Contrato, mediante cláusulas e condições seguintes:

CLÁUSULA PRIMEIRA – DO FUNDAMENTO LEGAL.
1.1. O presente Contrato fundamenta-se:
1.1.1. nas determinações estabelecidas na Lei Federal nº. 8.666 de 21 de junho de 1993 com suas alterações, a Lei Federal nº. 10.520 de 17 de julho de 2002 que regulamenta a modalidade Pregão, Decreto Federal nº. 10.024 de 20 de setembro de 2019, Lei Complementar nº. 123, de 14 de dezembro de 2006 com as alterações contidas na Lei Complementar nº 147 de 07 de agosto de 2014.
1.1.2. nos preceitos de direito público; e
1.1.3. supletivamente, nos princípios da teoria geral dos contratos e nas disposições do direito privado.

CLÁUSULA SEGUNDA – DA VINCULAÇÃO DO CONTRATO.
2.1. O cumprimento deste Contrato vincula-se ao que consta:
2.1.1. no Edital e seus Anexos do Pregão Eletrônico nº __.__.__/____;
2.1.2. nos termos da proposta firmada pela CONTRATADA que, simultaneamente:
a) constem no Processo Administrativo nº __.__.__/____;
b) não contrariem o interesse público.

CLÁUSULA TERCEIRA – DO OBJETO.
3.1. O presente Contrato tem como objeto o _____ de acordo com as especificações constantes do Quadro I do Anexo I do Edital do Pregão Eletrônico nº __.__.__/____, que passa a integrar o presente Contrato independentemente de transcrição.
3.2. A CONTRATADA declara que sua proposta contempla todos os elementos necessários à sua execução, não podendo alegar durante a execução do presente Contrato, a falta de algum elemento necessário a perfeita execução do objeto contratado.

CLÁUSULA QUARTA – DO PRAZO DE VIGÊNCIA.
4.1. O Contrato terá vigência a partir da data de sua assinatura, tendo validade por 12 (doze) meses.
4.2. Os prazos de vigência deste contrato poderão ser prorrogados nos termos da Lei nº 8.666/1993.

CLÁUSULA QUINTA – DO VALOR.
5.1. O valor global estimado do presente Contrato é de R$ ___ (_____).

ITEM	ESPECIFICAÇÕES	QUANT.	UNID.	VALOR UNIT.	VALOR TOTAL

5.2. O valor do item acima, bem como o valor unitário, é o constante da proposta da CONTRATADA, vencedora do Pregão Eletrônico nº __.__.__/____, que passa a integrar o presente Contrato.
5.3. Por se tratar de estimativas, o valor constante da **cláusula 5.1** não constitui, em hipótese alguma, compromisso futuro para o CONTRATANTE, razão pela qual não poderão ser exigidos nem considerados como valores para pagamento mínimo, podendo sofrer alterações de acordo com as necessidades do CONTRATANTE, sem que isso justifique qualquer indenização à CONTRATADA.
5.4. Os preços dos serviços serão aqueles constantes da Nota Fiscal apresentada pela CONTRATADA, as quais deverão ser devidamente certificadas pelo CONTRATANTE.

CLÁUSULA SEXTA – DOS PRAZOS, CONDIÇÕES, GARANTIA E LOCAL DE PRESTAÇÃO DOS SERVIÇOS DO OBJETO DA LICITAÇÃO.

6.1. O Contrato resultante da Presente Licitação deverá ser executado de acordo com as necessidades da Secretaria de requisitante conforme o prazo de validade do contrato, que será de 12 (doze) meses, a contar da data de assinatura deste instrumento, podendo ser prorrogado de acordo com as Conveniências do Município e de acordo com o Art. 57, inciso II, da Lei Federal 8.666/93 e suas demais alterações.
7.2. Obriga-se a CONTRATADA a manter durante toda a execução do contrato todas as condições de habilitação e qualificação exigidas para a contratação, devendo ainda:
a) Prestar os serviços dentro dos parâmetros e rotinas estabelecidos, em observância às normas legais e regulamentares aplicáveis e às recomendações aceitas pela boa técnica, podendo o MUNICÍPIO recusá-los caso não estejam de acordo com o previsto neste Edital/Contrato ou nas normas aplicáveis à matéria;
b) Reparar, corrigir ou refazer, substituir às suas expensas, no todo ou em parte, os serviços nos quais forem detectados defeitos, vícios ou incorreções resultantes da prestação dos serviços ou dos métodos empregados ou por terem sido executados em desacordo com as especificações, normas aplicáveis ou com a boa técnica; imediatamente ou no prazo estabelecido pelo MUNICÍPIO;
c) A prestar os serviços junto ao Município, correndo todas as despesas necessárias, como alimentação, estadias e deslocamentos para a consecução dos serviços por conta da CONTRATADA.
d) Os serviços deverão ser prestados junto as diversas Secretarias do município de Pindoretama-CE;
e) Serão recusados pela administração os serviços em desconformidade com o presente Termo de referência;
f) As prestações dos serviços licitados serão feitas de acordo com as necessidades administrativas, durante o prazo de contratação.
g) Aceitar nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até 25% (vinte e cinco por cento) do valor inicial atualizado do contrato, na forma do art. 65, parágrafos 1o e 2o da Lei no 8.666/93 e suas alterações posteriores.

CLÁUSULA SÉTIMA – DO ACOMPANHAMENTO E FISCALIZAÇÃO

7.1. A execução contratual será acompanhada e fiscalizada pelo(a) Secretaria Competente, através de servidor especialmente designado para este fim pela CONTRATANTE, de acordo com o estabelecido no art. 67, da Lei Federal nº 8.666/1993.
7.2. A fiscalização dos serviços deverá ser efetuada através de vistorias que ocorrerão a qualquer tempo.
7.3. A presença da fiscalização da Secretaria Competente, não elide nem diminui a responsabilidade da empresa contratada.
7.4. O representante do Contratante anotará em registro próprio todas as ocorrências relacionadas com a execução do Contrato, determinando o que for necessário à regularidade das faltas ou defeitos observados.

7.5. Havendo necessidade de correção de serviços contratados, a Contratada se compromete a corrigi-los e/ ou refazê-los sem ônus para o Contratante, devendo o Contratante proceder nova fiscalização.
7.6. As decisões e providências que ultrapassarem a competência do representante do Contratante deverão ser levadas aos seus superiores, em tempo hábil, para a adoção das medidas convenientes.

CLÁUSULA OITAVA – DA SUBCONTRATAÇÃO DE TERCEIROS

8.1. Serão aceitas subcontratações de outros bens e serviços para a execução do contrato original. Contudo, em qualquer situação, a CONTRATADA é a única e integral responsável pelo cumprimento global do contrato.
8.2. Em hipótese nenhuma, haverá relacionamento contratual ou legal da CONTRATANTE com os subcontratados.
8.3. A CONTRATANTE reserva-se o direito de vetar a utilização de subcontratações por razões técnicas ou administrativas, visando unicamente o perfeito cumprimento do contrato.

CLÁUSULA NONA – DAS OBRIGAÇÕES E RESPONSABILIDADES DA CONTRATADA

9.1. Prestar os serviços conforme especificações deste Edital, e em consonância com a proposta de preços apresentada, de forma parcelada e imediata após o recebimento da AF (Autorização de Fornecimento) e no local especificado na mesma.
9.2. Manter, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;
9.3. Providenciar a imediata correção das deficiências e/ou irregularidades apontadas pelo MUNICÍPIO;
9.4. Fornecer em comodato todos os equipamentos necessários para conexão como: fonte, cabos, modem etc.
9.5. Reparar, corrigir ou refazer, substituir às suas expensas, no todo ou em parte, os serviços nos quais forem detectados defeitos, vícios ou incorreções resultantes da prestação dos serviços ou dos métodos empregados ou por terem sido executados em desacordo com as especificações, normas aplicáveis ou com a boa técnica; imediatamente ou no prazo estabelecido pelo MUNICÍPIO;
9.6. A prestar os serviços junto ao Município, correndo todas as despesas necessárias, como alimentação, estadias e deslocamentos para a consecução dos serviços por conta da CONTRATADA.
9.7. Os serviços deverão ser prestados junto as diversas Secretarias do município de Pindoretama-CE;
9.8. Serão recusados pela administração os serviços em desconformidade com o presente Termo de referência;
9.9. As prestações dos serviços licitados serão feitas de acordo com as necessidades administrativas, durante o prazo de contratação.
9.10. Aceitar nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até 25% (vinte e cinco por cento) do valor inicial atualizado do contrato, na forma do art. 65, parágrafos 1o e 2o da Lei no 8.666/93 e suas alterações posteriores.
9.10.1 – O serviço deverá ser instalado, configurado, ativado e entregue em pleno funcionamento pelo licitante vencedor;
9.10.2 – O licitante deverá fornecer todos os equipamentos e acessórios necessários para o perfeito e total funcionamento dos serviços descritos, assim como as características do link (racks, roteadores, modems, etc.) sem ônus adicional para o Município;
9.10.3 – Toda manutenção, reparo e substituição dos equipamentos e acessórios fornecidos pelo licitante estarão a cargo da mesma, sem ônus para o Município;
9.10.4 – O licitante deverá fornecer o equipamento roteador/ONU/Radio Antena (homologado pela ANATEL), cabendo a ela a responsabilidade de sua instalação, configuração e manutenção;
9.10.5 – O licitante deverá monitorar permanentemente o estado dos circuitos de comunicação de dados, abrindo imediatamente a solicitação de reparo do circuito em caso de falhas, degradação de performance ou evento que leve a indisponibilidade da rede e iniciando o processo de recuperação;
9.10.6 – Executar os serviços obedecendo à legislação vigente, notadamente aquela pertinente a efetivação das despesas públicas;
9.10.7 – Responsabilizar-se pela eficiência dos serviços, respondendo pelos danos e prejuízos decorrente de sua imperfeita ou negligente execução;
9.10.8 – Não transferir os serviços licitados a terceiros, salvo com a prévia e expressa anuência do Município;

9.10.9 – O serviço deverá estar disponível 24 (vinte e quatro) horas por dia, durante 07 (sete) dias da semana, podendo haver interrupções ou suspensões de natureza técnica/operacional, hipóteses em que haverá sempre informação prévia e justificada do licitante vencedor.
9.10.10 – A Central de Assistência Técnica da Contratada deverá estar à disposição para interação com a Contratante durante 8 (oito) horas por dia, 05 (cinco) dias por semana, todos os dias do ano com profissionais dedicados para este propósito;
9.11 - O tempo para atendimento aos chamados e execução dos serviços de manutenção técnica, quando acionados, deverão seguir o estipulado nas clausulas de SLA (Acordo de Nível de Serviço).

Comissão de Licitação
Folha Nº
307

CLÁUSULA DÉCIMA – DAS OBRIGAÇÕES E RESPONSABILIDADES DA CONTRATANTE

10.1. A Administração Pública obriga-se a:
10.1.1. Solicitar a execução do objeto à CONTRATADA através da emissão de Ordem de Serviço;
10.1.2. Utilizar os veículos locados de acordo com o manual de instruções de fábrica e/ou orientações da CONTRATADA;
10.1.3. Providenciar o empenho e posterior pagamento da Nota Fiscal e ou fatura em até 10 (dez) dias da data seguinte ao seu recebimento pelo CONTRATANTE, desde que o veículo esteja em perfeito estado de funcionamento, salvo nos caso em que eventual falha no bem tenha sido causada pelo CONTRATANTE, ocasião em que o pagamento dar-se-á devido, na forma contratada;
10.1.4. Cientificar a CONTRATADA, por escrito, de qualquer anormalidade constatada com o veículo locado/prestação de serviço, para as providências cabíveis;
10.1.5. Aplicar as penalidades previstas no Edital e seus anexos, na ata de registro de preços, no contrato e nas demais cominações legais, na hipótese de a CONTRATADA não cumprir os termos contratuais, mantidas as situações normais de disponibilidade e volume dos serviços, arcando a referida empresa com quaisquer prejuízos que tal ato acarretar ao CONTRATANTE;
10.1.6. Prestar à CONTRATADA todas as informações e dados por ela solicitados, desde que disponíveis e do conhecimento do CONTRATANTE, completando-os com cópias de análises, correspondências, instruções e documentos, quando pertinentes ao assunto objeto deste Contrato;
10.1.7. Garantir instalações para a guarda e estacionamento dos veículos envolvidos;
10.1.8. Responsabilizar-se pelo abastecimento de combustível do veículo contratado durante o tempo da prestação do serviço;
10.1.9. Informar a CONTRATADA, o dia a hora que os veículos devam ser disponibilizados;
10.1.10. Fiscalizar a execução do objeto através de sua unidade competente, podendo, em decorrente, solicitar providências da CONTRATADA, que atenderá ou justificará de imediato.

CLÁUSULA DÉCIMA PRIMEIRA – DAS SANÇÕES ADMINISTRATIVAS

11.1. Caso o licitante vencedor se recuse injustificadamente a assinar o contrato ou não apresente situação regular, no ato da assinatura do mesmo, será convocado outro licitante, observada a ordem de classificação, para celebrar o contrato, e assim sucessivamente, sem prejuízo da aplicação de multa de 10% (dez por cento) incidente sobre o valor a ser indenizado.
11.2. O licitante que convocado dentro do prazo de validade da sua proposta, não celebrar o contrato, deixar de entregar ou apresentar documentação falsa exigida para o certame, ensejar o retardamento da execução de seu objeto, não mantiver a proposta, comportar-se de modo inidôneo ou cometer fraude fiscal, ficará impedido de licitar e contratar com o Município de Pindoretama e será descredenciado no Cadastro de Licitações da Prefeitura Municipal de Pindoretama, pelo prazo de até 05 (cinco) anos, sem prejuízo das multas previstas no Edital e seus anexos, no contrato e nas demais cominações legais.
11.3. Aos proponentes que ensejarem o retardamento da execução contratual, seja total ou parcial, comportar-se de modo inidôneo, não mantiverem a proposta, fizerem declaração falsa ou cometerem fraude fiscal, falharem ou fraudarem na execução do contrato poderão ser aplicadas, conforme o caso, as seguintes sanções, sem prejuízo da reparação dos danos causados ao Município de Pindoretama pelo infrator:
I. Advertência;

II. Multa de até 10% (dez por cento) sobre o valor previsto da contratação. No caso de descumprimento do contrato firmado;
III. Suspensão temporária de participação em licitação e impedimento de contratar com o município de Pindoretama por prazo não superior a 02(dois) anos;
IV. Declaração de inidoneidade para licitar ou contratar com o município de Pindoretama 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 o contratado ressarcir o município de Pindoretama pelos prejuízos resultantes e após decorrido o prazo da sanção aplicada com base no inciso anterior.
11.4. O valor da multa aplicada será deduzido pela CONTRATANTE por ocasião do pagamento, momento em que o Departamento Administrativo e Financeiro do Município de Pindoretama comunicará à CONTRATADA;
11.5. Se não for possível o pagamento por meio de desconto, a CONTRATADA ficará obrigada a recolher a multa por meio de DAM – Documento de Arrecadação Municipal. Se não o fizer, será encaminhado ao órgão competente para cobrança e processo de execução.
11.6. A reabilitação do Contratado só poderá ser promovida, mediante requerimento, após decorrido o prazo da aplicação da sanção e desde que indenize o Município pelo efetivo prejuízo causado ao Erário quando a conduta faltosa, relativamente ao presente certame, repercutir prejudicialmente no âmbito da Administração Pública Municipal.
11.7. As sanções previstas serão aplicadas assegurando ao Contratado ou ao Adjudicatário, o contraditório e a ampla defesa, nos seguintes prazos e condições:
a) 05(cinco) dias úteis nos casos de advertência.
b) 10(dez) dias úteis da abertura de vista do processo, no caso de declaração de impedimento para licitar ou contratar com o Município de Pindoretama.
11.8. Nenhuma sanção será aplicada sem o devido processo administrativo, que prevê defesa prévia do interessado e recurso nos prazos definidos em lei, sendo-lhe franqueada vista ao processo.
11.9. A aplicação das penalidades é de competência do Secretário(a) signatário(a) do respectivo contrato.
11.10. As multas não têm caráter indenizatório e seu pagamento não eximirá a contratada de ser acionada judicialmente pela responsabilidade civil derivada de perdas e danos junto à CONTRATANTE, decorrentes das infrações cometidas.

CLÁUSULA DÉCIMA SEGUNDA – DA DOTAÇÃO ORÇAMENTÁRIA.
12.1. As despesas decorrentes do presente Contrato correrão por conta da seguinte dotação orçamentária: ____.

CLÁUSULA DÉCIMA TERCEIRA – DO PAGAMENTO
13.1. Os pagamentos serão realizados até **30 (trinta) dias** corridos após a apresentação da Nota Fiscal/Fatura devidamente atestada pelo setor competente e acompanhada dos seguintes documentos:
a) Certidão Negativa de Débitos Relativos aos Tributos Federais e à Dívida Ativa da União;
b) Certidão Negativa de Débitos junto aos Governos Estadual e Municipal;
c) Certificado de Regularidade do FGTS – CRF;
d) Certidão Negativa de Débitos Trabalhistas – CNDT.
13.2. Constatada qualquer divergência ou irregularidade na documentação, esta será devolvida à CONTRATADA para as devidas correções.
13.3. O pagamento fica condicionado à comprovação de que a CONTRATADA se encontra adimplente com a Regularidade Fiscal e Trabalhista.

Comissão Licitação
Folha Nº
308

CLÁUSULA DÉCIMA QUARTA – DO REGIME DE EXECUÇÃO DO SERVIÇO
14.1. Será executado em regime de empreitada por preço unitário, conforme a necessidade.

CLÁUSULA DÉCIMA QUINTA – DOS ACRÉSCIMOS OU SUPRESSÕES.

15.1. No interesse do CONTRATANTE, o valor inicial atualizado do Contrato poderá ser aumentado ou suprimido até o limite de 25% (vinte e cinco por cento), conforme disposto nos parágrafos 1° e 2° do art. 65 da Lei n° 8.666/93.

15.2. A CONTRATADA fica obrigada a aceitar, nas mesmas condições licitadas, os acréscimos ou supressões que se fizerem necessários.

15.3. Nenhum acréscimo ou supressão poderá exceder o limite estabelecido na **cláusula 15.1**, deste termo, exceto as reduções resultantes de acordo entre as partes.

CLÁUSULA DÉCIMA SEXTA – DA RESCISÃO CONTRATUAL.

16.1. A inexecução total ou parcial do Contrato por qualquer dos motivos constantes do art. 78 da Lei n° 8.666/93 é causa para sua rescisão, na forma do art. 79 e com as consequências previstas no art. 80, do mesmo diploma legal.

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

16.3. No procedimento que visa à rescisão de Contrato, será assegurado o contraditório e a ampla defesa no prazo de 5 (cinco) dias, sem prejuízo da possibilidade de o CONTRATADO adotar motivadamente, providências acauteladoras.

CLÁUSULA DÉCIMA SÉTIMA – DA ALTERAÇÃO DO CONTRATO.

17.1. O Contrato poderá ser alterado nos casos previstos no art. 65 da Lei n° 8.666/93, desde que haja interesse do CONTRATANTE com a apresentação das devidas justificativas e formalizadas em processo.

CLÁUSULA DÉCIMA OITAVA – DA PUBLICAÇÃO.

18.1. Em conformidade com o disposto no Parágrafo único do artigo 61 da Lei n° 8.666/93, o presente Contrato será publicado no Quadro de Avisos da Unidade Gestora, na forma de extrato.

CLÁUSULA DÉCIMA NONA – DO FORO.

19.1. As questões decorrentes da execução deste instrumento, que não possam ser dirimidas administrativamente, serão processadas e julgadas no foro da cidade de Pindoretama/CE, como o único capaz de dirimir as questões decorrentes do presente Contrato, com a exclusão de qualquer outro, por mais privilegiado que seja caso não sejam resolvidas administrativamente.

E, por estarem de acordo com o ajustado, as partes assinam o presente instrumento, após lido e achado conforme perante as testemunhas que também assinam, em duas vias, de igual teor, para um só efeito jurídico.

Pindoretama/CE, _____ de _____ de ____.

Comissão de Licitação
Folha Nº
309

_____

CONTRATANTE

_____

CONTRATADA

TESTEMUNHAS:

1. _____
CPF:

2. _____
CPF: