	WAN deve suportar IPv6; Deve suportar balanceamento de tráfego por sessão; Deve suportar o uso de DDNS, para casos onde uma ou ambas as pontas possuam IPs dinâmicos; Deve possuir suporte e estar licenciamento para uso de VRFs; A solução de SD-WAN pode ser fornecida em composição com o firewall, desde que atenda aos mesmos requisitos de performance; **GARANTIA E SUPORTE PARA A SOLUÇÃO DE NEXT GENERATION FIREWALL**: Deve possuir garantia mínima, pelo fabricante, incluindo, suporte, correções, manutenções e serviços de assistência técnica, de 36 (trinta e seis) meses na modalidade 24x7; **SERVIÇOS DE INSTALAÇÃO:** Deverá ser realizada reunião inicial de projeto, com o objetivo de planejar a arquitetura da solução, instalação dos equipamentos, nivelar os entendimentos acerca das condições estabelecidas no Edital e em seus anexos, e esclarecer possíveis dúvidas; Identificação dos ativos de rede da CONTRATANTE que serão interconectados com a solução da adquirida, incluindo informações sobre interconexões lógicas, físicas e endereçamento interno dos seguimentos de rede; Detalhamento das ações necessárias para implementação da solução ofertada; Os equipamentos deverão ser entregues e instalados em alta disponibilidade no Datacenter da CONTRATANTE; O planejamento da implementação da Solução ofertada deverá ser iniciado 5 dias após a entrega dos equipamentos; Realizar Validação do hardware; Realizar formatação e update do firewall; Realizar configuração inicial do Firewall: Registrar; Configurar disco do firewall (Se for presente); Configurar portas de acesso e serviços; Configurar Interfaces; Configurar rotas para os gateways; Alterar o nome do firewall; Definir servidor de horário; Criar os usuários Administradores; Configurar os Logs; Ativar/Desativar features; Configurar update das soluções por subscrição Realizar configuração de usuários: Configurar agent do Single SignOn com a Active Directory: Configurações iniciais do agente; Definir e criar grupos de navegação; Linkar no agent os grupos; Configurar no firewall a comunicação entre o agente; Criar os grupos no firewall linkando os grupos do agent: Método LDAP; Método SSOAD; Realizar configuração de filtros UTM Antivírus; Criar os perfis de antivírus; Modo flow; Modo proxy; WebFilter; Criar os perfis referentes aos grupos; Ajustar as configurações de cada grupo; ApplicationControl; Criar os perfis referentes aos grupos; Ajustar as configurações de cada grupo; IntrusionProtection; Criar os perfis de IPs: Proteção de cliente; Caso necessário para algum servidor criar perfil específico; Realizar a criação dos objetos: Rede local; Grupos: Servidores; Máquinas Liberadas; Máquinas Bloqueadas; Destinos confiáveis: Virtual IPs (NATs); Criar os NATs utilizando porta ou origem; Realizar a criação das policies; Algumas policies serão criadas baseando-se nas		

	existentes no antigo firewall da CONTRATANTE; Regras não autenticadas; Regras autenticadas; Realizar a configuração da VPN SSL; Realizar configuração e integração com a Gerência de Logs e Relatórios; Configuração da solução de gerência de relatórios e logs; Instalação e configuração do appliance virtual; Criação e configuração de pelo menos os seguintes relatórios: Aplicações; Segurança; Sistema; Usuários; Web.		
Acess Point	**Caracteristicas Gerais:** Deve possuir garantia e suporte pelo período de 36 (trinta e seis) meses. Ponto de acesso (AP) que permita acesso dos dispositivos à rede através da rede sem fio e que possua todas as suas configurações centralizadas em controlador wireless; Deve suportar modo de operação centralizado, ou seja, sua operação depende do controlador wireless que é responsável por gerenciar as políticas de segurança, qualidade de serviço (QoS) e monitoramento da radiofrequência; Deve identificar automaticamente o controlador wireless ao qual se conectará; Deve permitir ser gerenciado remotamente através de links WAN; Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax de forma simultânea; Deve possuir capacidade dual-band com rádios 2.4GHz e 5GHz operando simultaneamente, além de permitir configurações independentes para cada rádio; O ponto de acesso deve possuir rádio Wi-Fi adicional a aqueles que conectam clientes para funcionar exclusivamente como sensor Wi-Fi com objetivo de identificar interferências e ameaças de segurança (wIDS/wIPS) em tempo real e com operação 24x7. Caso o ponto de acesso não possua rádio adicional com tal recurso, será aceita composição do ponto de acesso e hardware ou ponto de acesso adicional do mesmo fabricante para funcionamento dedicado para tal operação; Deve possuir rádio BLE (Bluetooth Low Energy) integrado e interno ao equipamento; Deve permitir a conexão de 400 (quatrocentos) clientes wireless simultaneamente; Deve possuir 2 (duas) interfaces Ethernet padrão 10/100/1000Base-T com conector RJ-45 para permitir a conexão com a rede LAN; Deve implementar link aggregation de acordo com o padrão IEEE 802.3ad; Deve possuir interface console para gerenciamento local com conexão serial padrão RS-232 e conector RJ45 ou USB; Deve permitir sua alimentação através de Power Over Ethernet (PoE); Adicionalmente, o ponto de acesso deve suportar modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser tunelados até o controlador wireless; Deve permitir operação em modo Mesh; Deve possuir potência de irradiação mínima de 21dBm em	Und	12

	ambas as frequências; Deve suportar, no mínimo, operação MIMO 2x2 com 2 fluxos espaciais permitindo data rates de até 1100 Mbps em um único rádio; Deve suportar MU-MIMO com operações em Downlink (DL) e Uplink (UL); Deve suportar modulação de até 1024 QAM para os rádios que operam em 2.4 e 5GHz servindo clientes wireless 802.11ax; Deve suportar recurso de Target Wake Time (TWT); Deve suportar BSS Coloring; Deve suportar operação em 5GHz com canais de 20, 40 e 80MHz; Deve possuir antenas internas ao equipamento com ganho mínimo de 4dBi em 2.4GHz e 5GHz; Em conjunto com o controlador wireless, deve otimizar o desempenho e a cobertura wireless (RF), realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados; Em conjunto com o controlador wireless, deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz; Em conjunto com o controlador wireless, deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz; Deve suportar mecanismos para detecção e mitigação automática de pontos de acesso não autorizados, também conhecidos como Rogue Aps; Em conjunto com o controlador wireless, deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless (wIDS/wIPS); Em conjunto com o controlador wireless, deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível criar até 14 (quatorze) SSIDs com operação simultânea; Em conjunto com o controlador wireless, deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES); Em conjunto com o controlador wireless, deve ser compatível e implementar o método de autenticação WPA3; Em conjunto com o controlador wireless, deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS; Deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP; Deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming; Deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming; Deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos; Deve		

	implementar o padrão IEEE 802.11e; Deve implementar o padrão IEEE 802.11h; Deve implementar o padrão IEEE 802.3az; Deve suportar ser gerenciado via SNMP; Deve suportar consultas via REST API; Deve possuir estrutura robusta para operação em ambientes internos e permitir ser instalado em paredes e tetos. Deve acompanhar os acessórios para fixação; Deve ser capaz de operar em ambientes com temperaturas entre 0 e 45º C; Deve possuir sistema antifurto do tipo Kensington Security Lock ou similar; Deve possuir indicadores luminosos (LED) para indicação de status; O ponto de acesso deverá ser compatível e ser gerenciado pelos controladores wireless deste processo; Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; Deve possuir certificado emitido pela Wi-Fi Alliance; Deve estar homologado pela ANATEL na data de execução do pregão; Deverá ser compatível e integrável com controladora Wireless descrita no item "2.10" ou ser compatível e gerenciado pelo Item "01" deste termo ou por solução em alta disponibilidade do mesmo fabricante.		
Controladora de Rede sem Fio	A solução de controladora sem fio deverá administrar e controlar de maneira centralizada os pontos de acesso wireless do mesmo fabricante da solução ofertada a fim de garantir uma perfeita interoperabilidade, podendo ser fornecida de forma integrada e agregada com outras soluções fornecidas nesse processo, desde que atenda todas as especificações técnicas descritas nesse item; Deve ser fornecido na forma de appliance físico composto pelo conjunto de hardware e software; Deve possuir pelo menos 2 (duas) interfaces 10 Gigabit Ethernet padrão 10GBase-X para permitir a conexão com a rede LAN. Adicionalmente devem ser fornecidos 2 (duas) transceivers SFP+ conforme padrão 10GBase-SR; Deve possuir interface console com conector RJ-45 ou USB para gerenciamento local; Deve possuir fonte de alimentação com capacidade de operação em tensões de 100 até 240VAC. Deve acompanhar o cabo de alimentação; Deve suportar a instalação de fonte de alimentação redundante; Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; A solução deve estar pronta e licenciada para garantir o gerenciamento de até 500 (quinhentos) pontos de acesso wireless simultaneamente em um único appliance; Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax; Deve permitir a conexão de dispositivos wireless que transmitam tráfego IPv4 e IPv6; A solução deverá ser capaz de gerenciar pontos de acesso do tipo indoor e outdoor; A solução deverá ser capaz de gerenciar pontos de acesso que estejam conectados remotamente através de links WAN e	Und	01

	Internet; O contrador wireless deve permitir ser descoberto automaticamente pelos pontos de acesso através de Broadcast, DHCP e consulta DNS; A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário; Permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points; O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser tunelados até o controlador wireless. Caso o controlador wireless não seja capaz de operar gerenciando os pontos de acesso e concentrando o tráfego tunelado simultaneamente, então a solução ofertada deve ser composta com elemento adicional para suportar a conexão dos túneis originados dos pontos de acesso; Quando o encaminhamento de tráfego dos clientes wireless for tunelado, para garantir a integridade dos dados, este tráfego deve ser enviado pelo AP para o concentrador através de túnel IPSec; Quando o encaminhamento de tráfego dos clientes wireless for tunelado, de forma a garantir melhor utilização dos recursos, a solução deve suportar recurso de Split-Tunneling por SSID. Com este recurso, o AP deve suportar a criação de listas de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes devem ser tunelados exceto aqueles que tenham como destino os endereços especificados nas listas de exceção; Adicionalmente, a solução deve suportar a configuração de SSIDs com modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser tunelados até o controlador wireless; Operando em Bridge Mode ou Local Switch, quando ocorrer falha na comunicação entre controladora e ponto de acesso os clientes devem permanecer conectados ao mesmo SSID para garantir a continuidade na transferência de dados, além de permitir que novos clientes sejam admitidos à rede, mesmo quando o SSID estiver configurado com autenticação 802.1X; A solução deve permitir definir quais redes serão tuneladas até o controlador e quais redes serão comutadas diretamente pela interface do ponto de acesso; A solução deve implementar recursos que possibilitem a identificação de interferências provenientes		

	de equipamentos que operem nas frequências de 2.4GHz e 5GHz; A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência; A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm; A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso; A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como Rogue APs. A mitigação deverá ocorrer de forma automática e baeada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados; A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN; A solução deve detectar os pontos de acesso não autorizados e/ou intrusos através de rádios dedicados para a função de análise ou através de Off-channel/Background scanning. Quando realizada através de Off-channel/Background scanning, a solução deve ser capaz de mensurar a utilização do ponto de acesso para, caso necessário, atrasar a análise e desta forma não prejudicar os clientes conectados; A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexbilidade no design da rede wireless; A solução deve permitir a adição de controlador redundante que deve monitorar a disponibilidade e sincronizar as configurações do controlador principal, além de assumir todas as funções em caso de falha do controlador primário. Desta forma, todos os pontos de acesso devem se associar automaticamente ao controlador redundante que passará a ter função de primário de forma temporária; A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP; A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com		

	configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado; A solução deve permitir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários; Deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio; A solução deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming; A solução deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming; A solução deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos; A solução deve implementar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless; A solução deve suportar priorização via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada; A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas; A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, Fabricante e sistema operacional do dispositivo, Endereço IP, SSID ao qual está conectado, Ponto de acesso ao qual está conectado, Canal ao qual está conectado, Banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação; Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering; A solução deve permitir a configuração de quais data rates estarão ativos na ferramenta e quais serão desabilitados; A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de Airtime; A solução deve suportar a configuração do BLE (Blueooth Low Energy) nos pontos de acesso que tenham este recurso; A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados; A solução deve suportar		

	recurso para automaticamente desconectar clientes wireless que estejam com sinal fraco ou distantes. Deve permitir definir o limiar de sinal para que os clientes sejam desconectados; A solução deve permitir a configuração de Short Guard Interval para o rádio 5GHz; A solução deve implementar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime nos SSIDs; A solução deve ser capaz de reconfigurar automaticamente os pontos de acesso para que desativem a conexão de clientes nos rádios 2.4GHz quando for identificado um alto índice de sobreposição de sinal oriundo de outros pontos de acesso gerenciados pela mesma infraestrutura, evitando assim interferências; A solução deve ser capaz de implementar regras de firewall stateful para controle do tráfego permitindo ou descartando pacotes de acordo com a política configurada, regras estas que devem usar como critérios dia e hora, endereços de origem e destino (IPv4 e IPv6), portas e protocolos; A solução deve permitir a configuração de regras de identity-based firewall, ou seja, deve permitir que grupos de usuários sejam utilizados como critério para permitir ou bloquear o tráfego; A solução deve implementar recurso para controle de URLs acessadas na rede wireless através de análise dos protocolos HTTP e HTTPS. Deve possuir uma base de conhecimento para categorização das URLs e permitir configurar quais categorias serão permitidas e bloqueadas de acordo com o perfil dos usuários e SSID; A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos websites acessados na rede wireless; O administrador da rede deve ser capaz de adicionar manualmente URLs e expressões regulares que deverão ser bloqueadas ou permitidas independente da sua categoria; A solução deve registrar todos os logs de eventos com bloqueios e liberações das URLs acessadas; A solução deve atualizar periodicamente e automaticamente a base de URLs durante toda a vigência do prazo de garantia da solução; A solução deve implementar solução de segurança baseada em filtragem do protocolo DNS com múltiplas categorias de websites/domínios pré-configurados em sua base de conhecimento; A ferramenta de filtragem do protocolo DNS deve garantir que o administrador da rede seja capaz de criar políticas de segurança para liberar, bloquear ou monitorar o acesso aos websites/domínios para cada categoria e também para websites/domínios específicos; A solução deve registrar todos os logs de eventos com bloqueios e liberações dos acessos aos websites/domínios que passaram pelo filtro de DNS; A ferramenta de filtragem do protocolo DNS deve identificar os domínios utilizados por Botnets para ataques do tipo Command & Control (C&C) e bloquear acessos e consultas oriundas da rede wireless com destino a estes domínios maliciosos. Os usuários não deverão ser capazes		

	de resolver os endereços dos domínios maliciosos através de consultas do tipo nslookup e/ou dig; O recurso de filtragem do protocolo DNS deve ser capaz de filtrar consultas DNS em IPv6; A solução deve possuir capacidade de reconhecimento de aplicações através da técnica de DPI (Deep Packet Inspection) que permita ao administrador da rede monitorar o perfil de acesso dos usuários e implementar políticas de controle para tráfego IPv4 e IPv6. Deve permitir o funcionamento deste recurso durante todo o período de garantia da solução; A solução deve registrar todos os logs de eventos com bloqueios e liberações das aplicações que foram acessadas na rede wireless; A solução deve atualizar periodicamente e automaticamente a base de aplicações durante toda a vigência do prazo de garantia da solução; A base de reconhecimento de aplicações através de DPI deve identificar, no mínimo, 2000 (duas mil) aplicações; A solução deve permitir a criação de regras para bloqueio e limite de banda (em Mbps, Kbps ou Bps) para as aplicações reconhecidas através da técnica de DPI; A solução deve permitir aplicar regras de bloqueio e limites de banda para, no mínimo, 10 aplicações de maneira simultânea em cada SSID; A solução deve ainda, através da técnica de DPI, reconhecer aplicações sensíveis ao negócio e permitir a priorização deste tráfego com marcação QoS; A solução deve monitorar e classificar o risco das aplicações acessadas pelos clientes wireless; "A solução deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless. Ao menos os seguintes ataques devem ser identificados: - Ataques de flood contra o protocolo EAPOL (EAPOL Flooding); - Os seguintes ataques de negação de serviço: Association Flood, Authentication Flood, Broadcast Deauthentication e Spoofed Deauthentication; - ASLEAP; - Null Probe Response or Null SSID Probe Response; - Long Duration; - Ataques contra Wireless Bridges; - Weak WEP; - Invalid MAC OUI." A solução deve implementar mecanismos de proteção para mitigar ataques à infraestrutura wireless. Ao menos ataques de negação de serviço devem ser mitigados pela infraestrutura através do envio de pacotes de deauthentication; A solução deve implementar mecanismos de proteção contra ataques do tipo ARP Poisoning na rede wireless; Permitir configurar o bloqueio na comunicação entre os clientes wireless conectados a um determinado SSID; Deve implementar autenticação administrativa através do protocolos RADIUS ou TACACS; Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES); Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3; A solução deve permitir a configuração de múltplas chaves de autenticação PSK para utilização em um determinado SSID; Quando		

	usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada; A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS; A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações 802.1X; Em conjunto com os pontos de acesso, a solução deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP; A solução deve implementar recurso para autenticação dos usuários através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informarem as credenciais válidas para acesso à rede; A solução deve permitir a hospedagem do captive portal na memória interna do controlador wireless; A solução deve permitir a customização da página de autenticação, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens; A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede; A solução deve permitir que a página de autenticação seja hospedada em servidor externo; A solução deve permitir a configuração do captive portal com endereço IPv6; A solução deve permitir o cadastramento de contas para usuários visitantes na memória interna. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada; A solução deve possuir interface gráfica para administração e gerenciamento das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução; Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado; A solução deve implementar recurso de DHCP Server (em IPv4 e IPv6) para facilitar a configuração de redes visitantes; A solução deve suportar o protocolo OSPF em IPv4 e IPv6 para compartilhamento de rotas dinâmicas entre a infraestrutura de rede LAN e WLAN; A solução deve identificar automaticamente o tipo de equipamento e sistema operacional utilizado pelo dispostivo conectado à rede wireless; A solução deve permitir que os usuários sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado; A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados; A solução deve permitir a configuração de rede Mesh entre pontos de acesso indoor e outdoor; A solução deve possuir recurso		

	para realizar testes de conectividade nos pontos de acesso a fim de validar se as VLAN estão apropriadamente configuradas no equipamento ao qual os APs estejam fisicamente conectados; A solução deve permitir ser gerenciada através dos protocolos HTTPS e SSH via IPv4 e IPv6; A solução deve permitir o envio dos logs para múltiplos servidores syslog externos; A solução deve permitir ser gerenciada através do protocolo SNMP, além de emitir notificações através da geração de traps; A solução deve permitir que softwares de gerenciamento realizem consultas diretamente nos pontos de acesso via protocolo SNMP; A solução deve incluir suporte para as RFCs 1213 (MIB II) e RFC 2665 (Ethernet-like MIB); A solução deve permitir a captura de pacotes na rede wireless e exporta-los em arquivos no formato .pcap; A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD; A solução deve apresentar graficamente a topologia lógica da rede, representar os elementos da rede gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles; A solução deve permitir o gerenciamento unificado e de forma gráfica para redes WiFi e redes cabeadas; A solução deve permitir a atualização de firmware do controlador wireless mesmo quando conectado remotamente; A solução deve permitir a identificação do firmware utilizado por cada ponto de acesso gerenciado e permitir a atualização via interface gráfica; A solução deve permitir a atualização de firmware individualmente nos pontos de acesso, garantindo a gestão e operação simultânea de pontos de acesso com firmwares diferentes; A solução deve possuir ferramentas de diagnósticos e debug; A solução deve enviar e-mail de notificação aos administradores da rede em caso de evento de indisponibilidade de um ponto de acesso; A solução deve suportar comunicação com elementos externos através de REST API; A solução deverá ser compatível e gerenciar os pontos de acesso deste processo;		

Justificativa para o Parcelamento ou Não: No processo licitatório, a adjudicação se dará por item, nos termos do art. 82, § 1º, da Lei nº 14.133/2021 e da Súmula/TCU 247. Dessa forma, será realizada licitação para aquisição **1)** Nobreak 700 VA – 20und; **2)** Impressora Etiqueta Argox – 03und; **3)** Servidor – 01und; **4)** Apliance de Backup – 01und; **5)** Switch 48 L2 – 05und; **6)** Switch 48 POE L3 – 01und; **7)** Next Generation Firewall (NGFW) – 01und**; 8)** Acess Point – 12und; **9)** Controladora de Rede sem Fio – 01und, em conformidade com o § 1º do art. 82 da Lei nº 14.133/2021. No entanto, a adjudicação se dará por itens, não havendo ofensa à Súmula nº 247 do TCU.

Contratações Correlatas e/ou Interdependentes: Não se aplica a esta contratação.

Benefícios a serem alcançados com a Contratação: Garantir uma assistência igualitária e de qualidade aos pacientes acompanhados nas diversas clínicas do Hospital Evangélico de Santa Maria de Jetibá, além de auxiliar na manutenção constante e aprimoramento do serviço prestado, proporcionando um acolhimento de ponta aos pacientes que buscam atendimento pelo Sistema Único de Saúde.

Providências a serem Adotadas: Não se vislumbra necessidades de tomada de providências de adequações para a solução a ser contratada.

Possíveis Impactos Ambientais: Não se vislumbra impactos ambientais para os itens que se pretende adquirir.

Declaração de Viabilidade da Contratação: Diante do exposto, declara-se viável a contratação pretendida, mostrando-se tecnicamente e fundamentadamente necessária, através deste Estudo Técnico Preliminar (ETP).

RESPONSÁVEL PELO ESTUDO TÉCNICO PRELIMINAR
Dree Elle Mendonça Freitas Lima
Fernanda Dalcolmo Coura Macedo

Análise de Riscos

Aquisição de Equipamentos de Informática – PE 022/2024

Fase de Análise – Planejamento da Contratação e Seleção da Contratada

RISCO 1 - Licitação Deserta ou Fracassada		
Probabilidade	**( ) Baixa (x) Média ( ) Alta**	
Impacto	**( ) Baixo (x) Médio ( ) Alto**	
Id	**Dano**	
1.	Não se concretiza a contratação pretendida	
	Ação preventiva	**Responsável**
1.	Elaborar descritivo detalhado do objeto a ser licitado	Gestor da Área Solicitante
2.	Efetuar pesquisa adequada de preços e análise de mercado em busca de maior número de participantes	Analista de Licitações/Equipe de Apoio
	Ação de contingência	**Responsável**
1.	Realizar nova licitação ampliando a divulgação e contactar fornecedores	Pregoeiro e Equipe de Apoio
RISCO 2 – Atraso na Liberação de Recurso		
Probabilidade	**(x Baixa ( ) Média ( ) Alta**	
Impacto	**( ) Baixo (x) Médio ( ) Alto**	
Id	**Dano**	
1.	Não se concretiza a contratação pretendida	
	Ação preventiva	**Responsável**
1.	Verificar se o recurso foi disponibilizado na conta bancária do Hospital antes da celebração de contrato	Analista de Licitações/Equipe de Apoio
	Ação de contingência	**Responsável**
1.	Monitorar e aguardar liberação de recurso em conta para celebração de contrato	Analista de Licitações/Equipe de Apoio
RISCO 3 – Dificuldade na Aquisição do Objeto Licitado		
Probabilidade	**( ) Baixa (x) Média ( )Alta**	
Impacto	**( )Baixo (x) Médio ( )Alto**	
Id	**Dano**	
1.	Não se concretiza a contratação pretendida	
	Ação preventiva	**Responsável**
1.	Efetuar pesquisa de mercado para verificar se o valor e descritivo do objeto estão condizentes com o mercado	Analista de Licitações/Equipe de Apoio
	Ação de contingência	**Responsável**
1.	Solicitar reformulação para ajuste do plano de trabalho, visando sanar o fator que está impedindo a aquisição do objeto ou substituir o item	Setor de Licitações

AEBES

PLANILHA DE CUSTOS

PROJETO: Assistência Integral ao Paciente Assistido pelo Hospital Evangélico de Vila Velha

PROPONENTE: AEBES - Associação Evangélica Beneficente Espírito Santense

META	ITEM	DISCRIMINAÇÃO	Unid	Qnt	PREÇOS		Total do Item
					Unitário	Total	
1	1.1	Colposcópio	Und	1	R$ 21.210,00	R$ 21.210,00	R$ 21.210,00
1	1.2	Foco Cirúrgico Móvel	Und	1	R$ 21.980,00	R$ 21.980,00	R$ 21.980,00
1	1.3	Carro para Medicação Beira Leito	Und	11	R$ 7.500,00	R$ 82.500,00	R$ 82.500,00
1	1.4	Freezer Horizontal	Und	1	R$ 2.948,00	R$ 2.948,00	R$ 2.948,00
1	1.5	Sistema de Vídeo Cirurgia/Laparoscopia	Und	1	R$ 368.000,00	R$ 368.000,00	R$ 368.000,00
1	1.6	Nobreak 700 VA	Und	20	R$ 588,92	R$ 11.778,40	R$ 11.778,40
1	1.7	Impressora Etiqueta Argox	Und	3	R$ 1.799,00	R$ 5.397,00	R$ 5.397,00
1	1.8	Biombo	Und	9	R$ 744,60	R$ 6.701,40	R$ 6.701,40
1	1.9	Poltrona Hospitalar	Und	15	R$ 1.320,00	R$ 19.800,00	R$ 19.800,00
1	1.10	Eletrocardiógrafo	Und	2	R$ 8.995,60	R$ 17.911,20	R$ 17.911,20
1	1.11	Carro de Curativo	Und	4	R$ 1.347,57	R$ 5.390,28	R$ 5,390,28
1	1.12	Suporte de Soro	Und	10	R$ 390,11	R$ 3.901,10	R$ 3.901,10
1	1.13	Carro Maca Avançado	Und	5	R$ 11.940,76	R$ 59.703,80	R$ 59.703,80
1	1.14	Ar Condicionado 36.000 BTUs	Und	2	R$ 9.081,90	R$ 18.163,80	R$ 18.163,80
1	1.15	Ar Condicionado 27.000 ou 30.000 BTUs	Und	1	R$ 7.409,05	R$ 7.409,05	R$ 7.409,05
1	1.16	Ar Condicionado 18.000 BTUs	Und	2	R$ 4.239,00	R$ 8.478,00	R$ 8.478,00
1	1.17	Ar Condicionado 12.000 BTUs	Und	7	R$ 2.390,11	R$ 16.730,77	R$ 16.730,77

META	ITEM	DISCRIMINAÇÃO	Unid	Qnt	PREÇOS		Total do Item
					Unitário	Total	
1	**1.18**	Ar Condicionado 9.000 BTUs	Und	7	R$ 2.190,10	R$ 15.330,70	R$ 15.330,70
1	**1.19**	Servidor	Und	1	R$ 72.588,75	R$ 72.588,75	R$ 72.588,75
1	**1.20**	Solução de Backup	Und	1	R$ 451.190,00	R$ 451.190,00	R$ 451.190,00
1	**1.21**	Switch 48 L2	Und	5	R$ 16.513,28	R$ 82.566,40	R$ 82.566,40
1	**1.22**	Switch 48 POE L3’	Und	1	R$ 33.909,94	R$ 33.909,94	R$ 33.909,94
1	**1.23**	Next Generation Firewall (NGFW)	Und	1	R$ 19.314,81	R$ 19.314,81	R$ 19.314,81
1	**1.24**	Acess Point	Und	12	R$ 10.711,18	R$ 128.534,13	R$ 128.534,13
1	**1.25**	Controladora de Rede sem Fio	Und	1	R$ 25.400,00	R$ 25.400,00	R$ 25.400,00
							TOTAL GERAL: R$ 1.506.837,53

Assinatura eletrônica
07/05/2024 07:36 UTC -03:00

ICP Brasil

Rodrigo André Seidel

CPF: 576.696.940-68
Rodrigo André Seidel

Rodrigo André Seidel
Presidente

Relatório de Assinaturas

ENVELOPE

Descrição do Envelope - 3 Planilha de Custos R$ 1504755,23 Equipamentos

ID do Envelope : 463188

Aponte a câmera do seu celular com leitor de QR CODE para verificar a validade das assinaturas deste envelope.

ARQUIVO

3 Planilha de Custos R$ 1.504.755,23 Equipamentos.pdf — 2 págs. PDF

Código de Verificação: db53c770-23ee-4591-9c92-f2ad0d305008
Hash: ae2424a434af4ce72f1750680e0ae7a6866cbdf0a587809b53c353ff9a670978

ASSINADO POR

Rodrigo André Seidel

Data e horário: 07/05/2024 às 07:36 • Fuso Horário: UTC -03:00
Assinado como: Signatário
Assinatura: Eletrônica

Assinatura eletrônica
07/05/2024 07:36 UTC -03:00

Rodrigo André Seidel

CPF: 576.696.940-68
Rodrigo André Seidel

E-mail: presidencia.contratos@aebes.org.br
CPF: 576.696.940-68
IP: 189.50.10.242
Geolocalização: -20.3325443, -40.3341293
Hash: d4795cfa166a00ced49f6b97abcf2f36bf707b15cf3b7019b7513302c522f3d0