

	TERMO DE REFERÊNCIA OU PROCESSO DE CONTRATAÇÃO Nº101/2024	Código: CONT.FR.0100		
		Data da Elaboração: 11/07/2019	Revisão: 013 15/02/2024	

ASSOCIAÇÃO EVANGÉLICA BENEFICENTE ESPÍRITO-SANTENSE, pessoa jurídica de direito privado de utilidade pública, inscrita no CNPJ sob nº 28.127.926/0002-42, estabelecida na Av. Paulo Pereira Gomes, s/n, Morada de Laranjeiras, Serra/ES, CEP 29.166-828, que atua como gestora do Hospital Estadual Dr. Jayme Santos Neves, torna público a realização do processo de contratação de empresa especializada para a **Prestação de Serviços de Infraestrutura de Rede Wi-Fi, com Fornecimento de Equipamentos para Transmissão do Sinal ARUBA**, do tipo Menor Preço, neste Termo de Referência nº 101/2024.

1. DISPOSIÇÕES PRELIMINARES:

I.	Data da Publicação: 24/06/2024 .
II.	Data de início do acolhimento das propostas: às 09:00h do dia 24/06/2024 . (Horário de Brasília)
III.	Data limite para o recebimento das propostas: às 09:00h do dia 04/07/2024 . (Horário de Brasília)
IV.	Abertura das propostas: às 09:01h do dia 04/07/2024 . (Horário de Brasília)
V.	Início da seção de disputa: às 15:00h do dia 05/07/2024 . (Horário de Brasília)
VI.	Endereço eletrônico para envio das propostas: <u>www.publinexo.com.br/privado/</u>
VII.	O resultado da contratação será divulgado através do site: <u>https://www.evangelicovv.com.br/institucional/129-briefings-hejsn</u>
VIII.	O envio da proposta para a prestação de serviços neste Termo de Referência importará no aceite total dos termos apresentados neste Termo de Referência e Minuta de Contrato em anexo.

2. DO OBJETO DA CONTRATAÇÃO

O presente Termo de Referência tem por objeto a contratação de empresa especializada para a **Prestação de Serviços de Infraestrutura de Rede Wi-Fi, com Fornecimento de Equipamentos para Transmissão do Sinal ARUBA**, para o Hospital Estadual Dr. Jayme Santos Neves.

- a) O serviço abrangerá as atividades de solução de controle de acesso, solução de gerência de hardware, controlador wlan hardware, pontos de acesso interno, ponto de acesso cabeado, conexão entre os pontos, rack, atendimento dos níveis de serviço e manutenção da rede, atuando em conjunto com os profissionais do HEJSN.

2.1 ESPECIFICAÇÕES DA CONTRATAÇÃO

2.1.1 A CONTRATADA deverá:

- a) Iniciar a prestação dos serviços no prazo de até 30 (trinta) dias, a contar da data de início da assinatura do contrato.
- b) Prestar os serviços de forma contínua ao HEJSN, em regime de 24/7.

- c) Prestar suporte e manutenção *on site* durante a vigência do contrato conforme SLA - Service Level Agreement (Acordo de Nível de Serviço - ANS), definido abaixo:

TIPO	INÍCIO DO ATENDIMENTO	PRAZO DE SOLUÇÃO
Serviço parado	2h	Máximo 4h
Sistema com problema ocasionando lentidão	4h	8h
Sistema com problema, mas sem prejudicar operação	12h	48h

- d) Disponibilizar canal de atendimento para abertura de chamados que poderá ser sistema, telefone ou e-mail, com geração de ticket com horário do atendimento e número único para acompanhamento da solução.
- e) Prestar toda configuração e apoio à CONTRATANTE;
- f) Possuir profissional com certificação técnica ACMP (Aruba Certified Mobile Professional), ou seja, na solução do mesmo fabricante do software;
- g) Atender às normas de qualidade e segurança vigentes;
- h) Fornecer produtos mediante solicitação de compra/reposição de estoque em 07 dias;
- i) Fornecer apoio técnico na utilização e manejo dos produtos/equipamento;
- j) Realizar substituição imediata dos equipamentos em casos de manutenções preventivas e corretivas;
- k) Comunicar ao cliente, com a devida antecedência ou de acordo com o nível de serviço qualquer anormalidade na prestação de serviço;
- l) Manter a prestação de serviço sem nenhum tipo de interrupção conforme acordado em contrato.

2.1.2 Não é permitida a subcontratação total ou parcial do objeto deste contrato, bem como sua cessão ou transferência, total ou parcial, pela CONTRATADA;

2.1.3 O sistema deverá conter:

I. SOLUÇÃO DE CONTROLE DE ACESSO

- a) Solução ARUBA WIFI com especificações mínimas conforme abaixo:

QUANTIDADE	DESCRIÇÃO
HARDWARE	
39	Aruba IAP-315 (RW) 802.11n/ac Dual 2x2:2/4x4:4 MU-MIMO Radio Integrated Antenna AP
39	PD-9001GR-AC 30W 802.3at PoE+ 10/100/1000 Ethernet Indoor Rated Midspan Injector
39	AP-220-MNT-W1W Flat Surface Wall/Ceiling White AP Basic Flat Surface Mount Kit
39	PC-AC-BR Brazil AC Power Cord
SERVICE	
39	Aruba 3Y FC NBD Exch IAP 315 SVC
SOFTWARE	
39	Aruba Central Device Management 1 Token 3 Year Subscription E-STU
39	Aruba Central Cloud Services 1 Token 3 Year Subscription E-STU

- b)** Solução de autenticação de usuários e dispositivos para controle de acesso à rede baseada em appliance ou software;
- c)** Suportar integração com bases de dados de usuários do tipo LDAP, Active Directory e SQL;
- d)** Implementar gerenciamento e aplicação de políticas de autorização de acesso de usuários com base em:
 - d.1)** Atributos do usuário autenticado;
 - d.2)** Hora do dia, dia da semana;
 - d.3)** Tipo de dispositivo utilizado;
 - d.4)** Localização do usuário;
 - d.5)** Tipo de autenticação utilizado.
- e)** Implementar funcionalidade de classificação automática de dispositivos ("Device profiling"), de forma a descobrir, classificar e agrupar os dispositivos conectados na rede;
- f)** Classificar, no mínimo, por sistema operacional e tipo de dispositivo (Ex. Apple, Samsung);
- g)** Possuir interface para construção de regras e categorias customizadas de classificação de dispositivos;
- h)** Permitir que o administrador cadastre manualmente um determinado dispositivo em uma categoria;
- i)** Possuir base de regras e categorias de dispositivos pré-configurada;
- j)** Suportar mecanismo de atualização das regras e categorias pré-configuradas;
- k)** Implementar os serviços de autenticação, profiling e autorização para no mínimo 170 usuários/dispositivos simultâneos. Caso exista licenciamento distinto para usuários/dispositivos da rede sem fio (wireless) e usuários/dispositivos da rede cabeada (wired), deverão ser fornecidas as duas licenças para o número total de usuários solicitados.
- l)** Possuir recursos integrados de AAA, permitindo que a solução possa ser utilizada como plataforma de autenticação (RADIUS);
- m)** Possuir suporte a TACACS+;
- n)** Possuir CA integrada, para geração de certificados para os dispositivos que forem se autenticar na rede;
- o)** Permitir que a solução faça consultas em bases SQL, com o objetivo de buscar informação a serem utilizadas durante o processo de autenticação dos usuários;
- p)** Possuir ferramenta para gerenciar os processos de credenciamento, autenticação, autorização e contabilidade de usuários visitantes através de um portal web seguro;
- q)** Suportar dispositivos visitantes conectados simultaneamente na rede via portal web;
- r)** Implementar a criação de grupos de autorizadores com privilégios distintos, por SSID, de criação de credenciais temporárias e atribuição de permissões de acesso aos clientes;

- s) Realizar a autenticação dos autorizadores em base externa do tipo Microsoft Active Directory ou LDAP e atribuir o privilégio ao autorizador de acordo com o seu perfil;
- t) Implementar as funcionalidades de geração aleatória de lotes de credenciais temporárias pré-autorizadas;
- u) Implementar a importação e exportação da relação de credenciais temporárias através de arquivos.txt ou csv;
- v) Permitir a criação de validade das credenciais, baseando o início da validade na criação da conta ou no primeiro login da conta;
- w) Permitir que o visitante crie sua própria credencial temporária ("self-service") através do portal web, sem a necessidade de um autorizador;
- x) Permitir a customização do formulário de criação de credenciais, a ser preenchido pelo autorizador ou pelo visitante, em caso de autosserviço, especificando quais informações cadastrais dos visitantes são obrigatórias ou opcionais;
- y) Permitir a customização do nível de segurança da senha temporária que será gerada ao visitante, especificando a quantidade mínima de caracteres e o uso de caracteres especiais em números para compor a senha;
- z) Exigir que o usuário visitante aceite o "Termo de uso da rede" a cada login ou apenas no primeiro login;
- aa) Permitir o envio das credenciais aos usuários registrados através de mensagens SMS (Short Message Service), e-mail e impressão local;
- bb) Todas as licenças deverão ser permanentes e perpétuas. Não serão aceitos licenciamento de recursos com prazos limitados de utilização;
- cc) Suportar em caso de necessidade futura controle de acesso à rede cabeada;
- dd) Possuir a possibilidade de configuração de VLAN de pré-autenticação onde os usuários se conectam a uma VLAN ao ligar a máquina e após efetuar o login a VLAN seja alterada de acordo com a política aplicada ao login do usuário;
- ee) O Hardware necessário para funcionamento do software de controle de acesso será fornecido pela empresa contratada, podendo ser servidor, uma máquina virtual, appliance ou em cloud, deverá possuir capacidade de hardware suficiente para executar todas as funcionalidades do projeto, deverá possuir fontes de alimentação e discos rígidos redundantes, deverá possuir suporte com tempo de solução de problemas de até 6 horas. Deverá fornecer as licenças de sistema operacional, caso seja necessário. Podendo optar por solução free.

II. SOLUÇÃO DE GERÊNCIA DE HARDWARE

- a) A Solução de Gerência da Rede Sem Fio deve ser fornecida como serviço;

- b)** Caso exista a possibilidade de fornecimento em Appliance Virtual, deve ser fornecido o servidor com a capacidade recomendada pelo fabricante, comprovada por documento oficial com todas as licenças incluídas, inclusive de sistema operacional e outras que sejam necessárias para o funcionamento do sistema;
- c)** Ser obrigatoriamente do mesmo fabricante dos pontos de acesso e controladores;
- d)** Permitir a configuração e gerenciamento através de browser padrão seguro HTTPS;
- e)** Ser capaz de gerenciar todos os APs e controladores WLAN;
- f)** Permitir que os eventos sejam gravados remotamente utilizando Syslog;
- g)** Prover organização hierárquica de equipamentos, permitindo que um equipamento receba as configurações lógicas e as replique a outros equipamentos;
- h)** Possuir capacidade de projeto automatizado de redes sem fio nos padrões 802.11a, 802.11b e 802.11g, 802.11n e 802.11ac, segundo a geografia do prédio (planta);
- i)** Considerar a área de cobertura e a banda por usuário desejada;
- j)** Possibilitar a importação de plantas baixas nos formatos .dwg e .jpg;
- k)** Permitir a visualização de alertas da rede em tempo real;
- l)** Permitir a visualização de eventuais áreas sem cobertura de RF (áreas de sombra);
- m)** Monitorar o desempenho da rede wireless, consolidando informações de rede tais como: níveis de ruído, relação sinal-ruído, interferência, potência desinal;
- n)** Possuir capacidade de listagem on-line da localização de usuário, endereço IP, endereço MAC, nível de potência de recepção e dados de associação e de autenticação 802.1x;
- o)** Possuir informação visual e gráfica, planta baixa dos andares, para:
 - o.1)** Visualização dos APs instalados, com estado de funcionamento;
 - o.2)** Visualização do mapa de calor de RF(Heatmap);
 - o.3)** Localização de ativos conectados à rede (equipamentos 802.11);
 - o.4)** Localização de rogue APs.
- p)** Caso esta funcionalidade não esteja disponível no sistema de gerência, deve ser fornecido software, do mesmo fabricante, para atender este item, contemplando toda a rede e com redundância 1+1.
- q)** Possuir capacidade de identificação e listagem dos rádios vizinhos e respectivos SSID/BSSID que podem ser percebidos por cada AP;
- r)** Possuir capacidade de configuração gráfica completa do Controlador WLAN e respectivos APs;

- s)** Possuir capacidade de geração de relatórios dos seguintes tipos:
 - s.1)** Visualização dos APs instalados, com estado de funcionamento;
 - s.1)** Listagem de clientes Wireless;
 - s.1)** Listagem de APs;
 - s.1)** Informações de Configuração dos Controladores WLAN;
 - s.1)** Utilização da rede;
 - s.1)** Detalhes dos APs não autorizados (rogues) detectados.

- t)** Suportar SSH, HTTP/HTTPS, SSL, Telnet;

- u)** Possuir ferramentas de debug e log de eventos para depuração e gerenciamento em primeiro nível;

- v)** Implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps;

- w)** Possuir suporte a MIB II, conforme RFC1213;

- x)** Implementar a MIB privativa que forneça informações relativas ao funcionamento do equipamento;

- y)** Possibilitar a obtenção da configuração do equipamento através do protocolo SNMP;

- z)** Possibilitar a obtenção via SNMP de informações de capacidade e desempenho da CPU, memória e portas;

- aa)** Possibilitar a gerência e identificação individualizada de cada AP remoto;

- bb)** Permitir a administração centralizada dos APs sem a necessidade de configurar os APs individualmente;

- cc)** Possibilitar a identificação de paredes e divisórias com respectivos níveis de atenuação por tipo (alvenaria, vidro, drywall e divisória);

- dd)** Possibilitar a importação de plantas baixas nos formatos gráficos (CAD, .dwg, .jpg, .gif e .png);

- ee)** Disponibilizar em painel gráfico de controle informações referentes à:
 - ee.1)** Visualização dos APs instalados, com estado de funcionamento;
 - ee.2)** Sistemas operacionais e tipos de dispositivos que estão se conectando a rede;
 - ee.3)** Informações sobre chamadas de voz, seus protocolos e qualidade delas;
 - ee.4)** Informações sobre os tipos de aplicações mais utilizados;
 - ee.5)** Informações sobre usuários conectados.

- ff)** Possuir informação sobre possíveis ameaças a rede detectadas pelos sistemas gerenciados;

- gg)** Possibilitar criação de regras de detecção de ameaças e correlacionar todos os dispositivos gerenciados.

III. CONTROLADOR WLAN HARDWARE

- a)** Solução baseada em hardware, virtual ou cloud o, do mesmo fabricante dos pontos de acesso e software de gerência;

- b) Não serão aceitos hardwares genéricos.
- c) Gerenciar, no mínimo, a quantidade de 40 pontos de acesso simultaneamente, com centralização das funcionalidades de autenticação;
- d) Permitir a conexão simultânea de, no mínimo, 2.000 clientes wireless;
- e) Permitir o armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior à queda de alimentação;
- f) Permitir gravação de múltiplas configurações no próprio equipamento;
- g) Possuir fonte de alimentação com seleção automática de tensão (100-240VAC);
- h) Permitir a gravação de eventos por meio do protocolo Syslog;
- i) Possuir capacidade de gerenciamento hierárquico, com possibilidade de definição de grupos de equipamentos e alteração das características de configuração do grupo sem a necessidade de configuração individual de cada equipamento;
- j) Acesso ao sistema através de cliente com browser padrão (HTTP, HTTPS, Java);
- k) Possuir LEDs para a indicação do status das portas e atividade;
- l) Permitir ser montado em rack padrão de 19 (dezenove) polegadas, incluindo todos os acessórios necessários;
- m) Ser acompanhado de todos os acessórios necessários para operacionalização do equipamento, tais como: softwares, cabos de console, cabos de energia elétrica, documentação técnica e manuais que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização do equipamento;
 - m.1) Caso a controladora não possua as interfaces de rede solicitadas, poderá ser ofertado um switch LAN com as características de portas de rede solicitadas, para cada controladora ofertada.
- n) Permitir operação em modo mesh;
- o) Permitir o uso de múltiplos SSIDs simultaneamente;
- p) Prover tempo de fast-roaming intra-switch inferior a 25milissegundos;
- q) Permitir conexão entre APs sem a necessidade de conexão cabeada, implementando assim uma rede padrão mesh;
- r) Prover tempo de fast-roaming inter-switch em camada 2 inferiores a 100 milissegundos;
- s) Suportar 802.11e com WMM, U-APSD eT-SPEC;

- t)** Gerenciar centralizadamente a autenticação de usuários;
- u)** Implementar protocolo de autenticação para controle do acesso administrativo ao equipamento com mecanismos de AAA;
- v)** Possuir base de dados de usuários interna para autenticação de usuários convidados/temporários (acesso guest);
- w)** Permitir autenticação em no mínimo os seguintes sistemas de base de dados de usuários Microsoft Active Diretor, Cisco ACS server, Free Radius, entre outros;
- x)** Realizar o provisionamento de usuários convidados (guests) através de interface Web por meio de um usuário administrativo com permissões mínimas, exclusivas para este fim;
- y)** Possuir suporte a autenticação IEEE 802.1X, com pelo menos os seguintes métodos EAP: EAP-MD5, PEAP/EAP- GTC, PEAP/EAP-MSCHAPv2, EAP-TLS com utilização de base de usuários interna ou servidor RADIUS externo;
- z)** Suportar as especificações abaixo:
 - z.1)** RFC2409;
 - z.2)** RFC2661;
 - z.3)** RFC2408;
 - z.4)** RFC3602;
 - z.5)** RFC3948;
 - z.6)** RFC2548.
- aa)** Suportar os seguintes métodos:
 - aa.1)** RFC2409;
 - aa.2)** EAP-PEAP
 - aa.3)** EAP-TLS
 - aa.4)** EAP-TTLS;
- bb)** Possuir suporte a autenticação IEEE 802.1X, com o método PEAP/EAP-GTC, e com utilização de base de usuários LDAP externa;
- cc)** Permitir a seleção / uso de servidor Radius ou LDAP com base no SSID;
- dd)** Suportar a autenticação de usuários conectados à rede cabeada através das portas do controlador;
- ee)** Possuir o recurso de EAP Offload para terminação do túnel EAP no próprio controlador;
- ff)** Suportar utilização de Portal Captivo externo ao controlador;
- gg)** Permitir a autenticação (através de endereço MAC, Portal Captivo ou IEEE 802.1X) de usuários conectados à rede WLAN (wireless) ou usuários conectados às portas cabeadas do controlador. Também deverá permitir a autenticação de usuário e de máquina por meio de IEEE802.1x;

- hh)** Oferecer recurso de Portal Captivo (Captive Portal) com suporte a múltiplos portais simultaneamente;
- ii)** Implementar associação dinâmica de usuário a VLAN, com base nos parâmetros da etapa de autenticação;
- jj)** Implementar Qualidade de Serviço com a marcação de pacotes utilizando Diffserv e suporte a 802.1p para QoS de rede;
- kk)** Possibilitar roaming com integridade de sessão, dando suporte a aplicações em tempo real, tais como, VoIP, VoWLAN, videoconferência, dentre outras;
- ll)** Permitir portais captivos externos a controladora;
- mm)** A controladora deve possuir funcionalidade de conexão Site to Site VPN utilizando padrão Ipsec.
- nn)** Caso a solução fornecida não possua a funcionalidade, será aceita solução de VPN adicional;
- oo)** Implementar segurança IEEE802.11i;
- pp)** Suportar a criptografia centralizada com os seguintes protocolos: AES-CCMP, TKIP e WEP;
- qq)** Suportar, no mínimo, 2000 VLANs;
- rr)** Implementar o protocolo 802.1w (Rapid Spanning Tree);
- ss)** Oferecer suporte a roteamento e switching de camadas L2 e L3;
- tt)** Suportar as especificações abaixo:
 - tt.1)** RFC 2328;
 - tt.2)** RFC2338;
 - tt.3)** RFC1027;
 - tt.4)** IEEE 802.1w;
 - tt.5)** RFC 1519.
- uu)** Possuir o recurso de criação de Pools de VLAN para permitir a escalabilidade de redes;
- vv)** Possuir servidor DHCP embutido;
- ww)** Suportar o protocolo VRRP para redundância de controladores;
- xx)** Suportar redundância de controladores conectados em camada 3;
- yy)** Suportar redundância de controladores nos modos:
 - yy.1)** 1+1;
 - yy.1)** N+1;
 - yy.1)** Ativo-Ativo;
 - yy.1)** Ativo-Standby.

- zz)** Oferecer os recursos de mobilidade entre VLANs para roaming de camada 2;
- aaa)** Oferecer os recursos de Proxy de endereços IP e Proxy DHCP para roaming entre redes (L3);
- bbb)** Implementar tagging de VLANs através do protocolo 802.1Q;
- ccc)** Implementar o protocolo 802.1d para Spanning Tree (STP);
- ddd)** O controlador WLAN poderá estar diretamente e/ou remotamente conectado aos APs por ele gerenciados, inclusive via roteamento nível 3 da camada OSI;
- eee)** Se um controlador WLAN falhar, os APs relacionados deverão se associar a um controlador WLAN alternativo de forma automática, não permitindo que a rede wireless se torne inoperante;
- fff)** Realizar a descoberta automática dos APs na infraestrutura wireless;
- ggg)** Permitir o controle dos APs mediante a conexão através de topologia MESH (WiFiMesh);
- hhh)** A rede MESH deverá oferecer comportamento determinístico da topologia da rede MESH;
- iii)** A rede MESH deverá prover auto-redundância das camadas física (RF) e Layer 2 com comportamento determinístico;
- jjj)** Permitir a conexão de APs de maneira remota e segura;
- kkk)** Conectar APs através de redes públicas e/ou privadas com garantia de segurança através de conexão criptografada;
- lll)** Permitir a propagação de SSIDs de maneira segura para qualquer AP legitimamente cadastrado na controladora, independentemente de onde este AP esteja conectado;
- mmm)** Permitir a autenticação do AP remoto através de certificado digital ou de usuário e senha cadastrados em servidor AD e Radius;
- nnn)** Gerenciar o tráfego dos APs centralizadamente;
- ooo)** Permitir o uso de, pelo menos, uma interface Ethernet com rede segmentada para gerenciamento;
- ppp)** Otimizar o desempenho e a cobertura da radiofrequência;
- qqq)** Ajustar automaticamente os canais de modo a otimizar a cobertura de rede e mudar as condições de RF baseado em performance;
- rrr)** Detectar interferência e ajustar parâmetros de RF, evitando problemas de cobertura e controle da propagação indesejada de RF;
- sss)** Implementar varredura de RF contínua, programada ou sob demanda, com identificação de APs ou clientes irregulares;

- ttt)** Implementar a tecnologia de "Channel load balancing", permitindo que clientes sejam automaticamente distribuídos entre Pontos de Acesso adjacentes operando em canais distintos, com o objetivo de balancear a carga entre os Pontos de Acesso;
- uuu)** Implementar a tecnologia de "Band Steering/Select", permitindo que clientes com suporte a faixa de frequência de 5GHz se conectem aos Pontos de Acesso utilizando, preferencialmente, a faixa de 5GHz;
- vvv)** Implementar varredura de RF nas bandas 802.11a, 802.11b, 802.11g, 802.11n e 802.11ac para identificação de ataques e APs intrusos não autorizados (rogues);
- www)** Realizar a varredura no canal de operação do AP sem impacto na performance da rede WLAN;
- xxx)** Permitir a varredura em todos os canais possíveis de RF para detecção e contenção de ameaças na rede WLAN;
- yyy)** Fazer a varredura dos espectros de 2,4 GHz e 5 GHz para localização e classificação de interferências não 802.11, análise de espectro, e evitá-las automaticamente;
- zzz)** Detectar áreas de sombra de cobertura e efetuar os devidos ajustes para sua correção, automaticamente;
- aaaa)** Ajustar, dinamicamente, o nível de potência e canal de rádio dos APs, de modo a otimizar o tamanho da célula de RF, garantindo a performance e escalabilidade;
- bbbb)** Permitir o controle de banda disponível (bandwidth contracts) por usuário ou através de perfis de usuários;
- cccc)** Possibilitar roaming com integridade de sessão, dando suporte a aplicações em tempo real, tais como, VoIP, VoWLAN, videoconferência, dentre outras;
- dddd)** Possuir mecanismo de controle de admissão de chamadas nos pontos de acesso (CAC);
- eeee)** A controlador de possuir funcionalidade de conexão Site to Site VPN utilizando padrão Ipsec. Caso a solução fornecida não possua a funcionalidade, será aceita solução de VPN adicional;
- ffff)** Possuir mecanismo automático de QoS para protocolos de voz (SIP, SVP e SCCP) utilizando inspeção automática de pacotes, sem a necessidade de fazer a marcação prévia (tagging) de pacotes;
- gggg)** Possuir solução de identificação de aplicações através de técnicas de análise de tráfego, provendo informações das aplicações mais utilizadas na interface gráfica;
- hhhh)** Permitir a criação de políticas de acesso baseadas nas aplicações, como por exemplo, o acesso a "redes sociais" terá um controle de banda de 2Mbps.
- iiii)** Apresentar informações gráficas referente a utilização de soluções de comunicações unificadas (UC) sobre a infraestrutura WLAN, de formar a apresentar informações referentes as chamadas realizadas e relações gráficas entre o nível de sinal recebido pelo usuário e a qualidade da chamada.

- jjj) Possuir a funcionalidade da utilização do protocolo Bonjour na infraestrutura, permitindo que os serviços divulgados via mDNS sejam controlados, filtrados e disponibilizados entre diferentes subnets, tornando assim possível a utilização em redes com múltiplas subnets e um número grande de dispositivos.

IV. SERVIÇOS DE INFRAESTRUTURA

- a) Todos os equipamentos de distribuição de sinal WIFI deverão ser interligados com cabo UTP cat. 6 com todas as conexões com conectores cat.6.
- b) A estrutura deverá toda ser organizada em patch panel cat6.
- c) Todos os pontos e equipamento deverão ser identificados com etiquetas com nomenclatura definida pela equipe de T.I. do HEJSN.
- c.1) Instalação de toda infraestrutura;
 - c.2) Lançamento de cabos UTP Cat 6;
 - c.3) Conectorização de cabos UTP Cat 6;
 - c.4) Lançamento de cabos elétricos;
 - c.5) Montagem de tomadas;
 - c.6) Identificação e testes;
 - c.7) ART;
 - c.8) Instalação de todos os pontos de acesso WIFI;
 - c.9) Instalação de pontos de rede;
 - c.10) Treinamento para a equipe de T.I. do HEJSN. Ele deverá abranger toda configuração e manutenção da solução, com no mínimo 10 horas de duração para no mínimo 4 funcionários.

V. QUANTIDADE:

LOCAL	QTD	COBERTURA
1 ANDAR - D	1	CENTRO DE ENSINO E PESQUISA
1 ANDAR - E	1	SALA DE TREINAMENTO
1 ANDAR - F	3	CTQ / UTQ
2 ANDAR - F	5	ACTI ADULTO
3 ANDAR - F	6	UTIN, UCIN, CO
4 ANDAR - F	4	MATERNIDADE
5 ANDAR - F	3	INTERNAÇÃO
6 ANDAR - F	4	INTERNAÇÃO
TERREO - C	1	CENTRO CIRURGICO
TERREO - D	5	PRONTO SOCORRO
TERREO - F	6	IMAGEM, AMBULATORIO, USI
TOTAL:	39	

3. DA VIGÊNCIA DO CONTRATO

O prazo de vigência do contrato será até o dia 30 novembro de 2028, conforme contrato de gestão firmado entre a Secretaria Estadual de Saúde do Estado do Espírito Santo – SESA e AEBES, a contar da data de assinatura do instrumento contratual.

Este contrato será imediatamente rescindido no caso de encerramento do Contrato de Gestão do Hospital Estadual Dr. Jayme Santos Neves, hipótese em que a AEBES não poderá ser responsabilizada ao pagamento de indenizações ou multas de qualquer natureza.

4. CRITÉRIO DE JULGAMENTO:

Menor Valor Global.

4.1 TETO ORÇAMENTÁRIO

O teto orçamentário será no valor de R\$ 6.000,00 (seis mil reais) mensais.

5. DA PARTICIPAÇÃO

As empresas que desejarem participar do Termo de Referência deverão, obrigatoriamente, cadastrar-se gratuitamente na plataforma eletrônica denominada PUBLInexo, através do link a seguir: www.publinexo.com.br/privado/.

5.1 Do Credenciamento na Plataforma

5.1.1 O registro no site, o credenciamento dos representantes que atuarão em nome da proponente e a senha de acesso, deverá ser obtido antes do prazo limite do recebimento das propostas. O cadastro e o acesso à plataforma são gratuitos.

5.1.2 Para participação do Termo de Referência na plataforma PUBLInexo, a proponente deverá utilizar a chave de acesso e senha fornecida através de cadastro no site: www.publinexo.com.br/privado/.

5.1.3 A proponente responderá integralmente por todos os atos praticados no Termo de Referência, por seus representantes devidamente credenciados, assim como pela utilização da senha de acesso ao sistema, ainda que indevidamente, inclusive por pessoa não credenciada como sua representante.

5.2 Da Proposta

5.2.1 A Proposta de preço deverá ser apresentada por meio eletrônico no endereço www.publinexo.com.br/privado/, em idioma nacional, com a identificação da empresa, sem emendas, rasuras ou entrelinhas, devidamente datada, e na qual constará obrigatoriamente:

- I. Nome;
- II. Razão ou Denominação Social;
- III. Endereço completo do proponente;
- IV. Identificação do signatário da proposta, sua função e cargo na empresa no campo Observações no ato do registro das propostas;
- V. CNPJ e Inscrição Estadual da empresa;

5.2.2 Junto com a proposta de preço, o interessado deverá apresentar os documentos alusivos à sua habilitação, nos termos do item 8 deste Termo de Referência, sob pena de eliminação do certame.

5.2.3 Caso haja discrepâncias entre o descritivo na plataforma e no Termo de Referência, prevalecerá sempre o descritivo do Termo de Referência;

5.2.4 Deverá constar Preços UNITÁRIOS, de forma clara e indubitosa, expresso em moeda nacional, apurada na data de apresentação da proposta, sem inclusão de encargo financeiro ou previsão inflacionária;

- I. Nesses preços deverão ser computadas todas as despesas, impostos e outros que envolvam o Fornecimento objeto deste Termo de Referência;
- II. Todos os preços da Proposta deverão ser apresentados na moeda corrente nacional (Real), utilizando-se até quatro casas decimais para os centavos, precedidos da vírgula que segue a unidade, desprezando-se as frações remanescentes.

5.2.5 O Responsável pelo certame, solicitará ao arrematante do lote, que encaminhe exclusivamente por meio do sistema e/ou e-mail, em até 02 (dois) dias úteis após o encerramento da disputa, a proposta adequada ao último lance ofertado após a negociação realizada, acompanhada, se for o caso, dos documentos complementares, quando necessários à confirmação daqueles exigidos neste Termo de Referência e já apresentados.

5.2.6 Após a negociação do preço, o Responsável pelo certame iniciará a fase de aceitação e julgamento da proposta.

5.2.7 Na hipótese de a proposta vencedora não ser aceitável ou a participante não atender às exigências para habilitação, o Responsável pelo certame examinará a proposta subsequente e assim sucessivamente na ordem de classificação, até a apuração de uma proposta que atenda ao Termo de Referência.

5.3 Do Procedimento

5.3.1 O Ato Convocatório será processado e julgado com observância dos seguintes procedimentos:

- I. No dia e horário indicado neste ato Convocatório será aberta a sessão do Termo de Referência, com a abertura automática das propostas e sua divulgação, pelo sistema, na forma de grade ordenatória;
- II. A análise das propostas visará ao atendimento das condições estabelecidas neste Ato Convocatório e seus anexos, sendo desclassificadas as propostas:
 - a) cujo objeto não atenda as especificações, prazos e condições fixados no Ato Convocatório; e
 - b) que apresentem preço baseado exclusivamente em proposta das demais proponentes.
- III. No tocante aos preços, as propostas serão verificadas quanto à exatidão das operações aritméticas que conduziram ao valor total orçado, procedendo-se às correções no caso de eventuais erros, tomando-se como corretos os preços unitários. As correções efetuadas serão consideradas para apuração do valor da proposta.
- IV. As propostas não desclassificadas serão selecionadas para a etapa de lances.
- V. Será iniciada a etapa de lances, com a participação de todas as proponentes detentoras de propostas classificadas.
- VI. Os lances deverão ser formulados exclusivamente por meio eletrônico e em valores distintos e decrescentes, inferiores à proposta de menor preço, observada a redução mínima entre os lances de acordo com o critério do responsável pelo presente processo (decrécimo), aplicável inclusive em relação ao primeiro colocado.

- VII. A etapa de lances será considerada encerrada após o prazo determinado pelo responsável pelo presente processo e após a execução do tempo randômico. O Responsável não terá controle sobre o tempo randômico, ou seja, o sistema se encerrará automaticamente e aleatoriamente sem a intervenção humana.
- VIII. A aceitabilidade será aferida a partir dos preços de mercado vigentes na data da apresentação das propostas, apurados mediante pesquisa realizada pelo departamento de compras da instituição.

5.4 Da Desconexão do Sistema Eletrônico

5.4.1 À proponente caberá acompanhar as operações no sistema eletrônico, durante a sessão, respondendo pelo ônus decorrente de sua desconexão ou da inobservância de quaisquer mensagens emitidas pelo sistema.

5.4.2 No caso de desconexão do responsável pelo presente processo, no decorrer da etapa de lances, se o sistema eletrônico permanecer acessível aos proponentes, os lances continuarão sendo recebidos, sem prejuízo dos atos realizados.

5.5.3 Quando a desconexão do responsável pelo presente processo persistir por tempo superior a dez minutos, a sessão na forma eletrônica será suspensa e reiniciada somente após comunicação aos participantes, no endereço eletrônico utilizado para divulgação.

6. CRITÉRIO ELIMINATÓRIO

- I. Envio da proposta fora do prazo estabelecido nas disposições preliminares do presente termo ou em desacordo com o objeto da contratação.
- II. Ausência do envio de qualquer dos documentos obrigatórios descritos no item 8.

7. CRITÉRIO DE DESEMPATE

Melhor técnica (fornecimento de itens que estão além dos serviços solicitados).

8. DA HABILITAÇÃO OBRIGATÓRIA

Para habilitação, exigir-se-á dos interessados, exclusivamente, documentação relativa a:

8.1. Habilitação Jurídica:

- I. Prova de inscrição no Cadastro Nacional de Pessoa Jurídica – CNPJ do Ministério da Fazenda;
- II. Registro comercial, no caso de empresa individual;
- III. Ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado, em se tratando de sociedades empresariais ou cooperativas e, no caso de sociedades por ações, acompanhado de documentos de eleição de seus administradores e alterações ou da consolidação respectiva, sendo que deles deverá constar, entre os objetivos sociais, a execução de atividades da mesma natureza ou compatível com o objeto deste Termo de Referência;
- IV. Inscrição do ato constitutivo, no caso de sociedades civis, acompanhada de prova de eleição da diretoria em exercício;
- V. Decreto de autorização, em se tratando de empresa ou sociedade estrangeira em funcionamento no País, e ato de registro ou autorização para funcionamento expedido pelo órgão competente, quando a atividade assim o exigir;

8.2. Qualificação Técnica:

- I. Alvará de localização, funcionamento e demais alvarás obrigatórios em relação ao ramo de atividade desenvolvida. (Exemplos: Alvará de vigilância sanitária e corpo de bombeiro);
- II. Certificado de responsabilidade e regularidade técnica da ACMP (Aruba Certified Mobile Professional);
- III. CNAE - Classificação Nacional de Atividades Econômicas, compatível com o objeto da contratação para qual será contratada;
- IV. Atestado(s) de Capacidade Técnica que comprovem capacidade de satisfazer a dois aspectos indispensáveis: quantidade – experiência em atender o volume de demandas de acordo com o objeto; e qualidade – habilidade técnica na prestação dos serviços do objeto, conforme ANEXO I

8.3. Regularidade fiscal e trabalhista

- I. Prova de regularidade para com a Fazenda Federal, Estadual e Municipal do domicílio ou sede da proponente, ou outra equivalente, na forma da lei;
- II. Certidão Negativa de Débitos Trabalhistas (CNDT), expedida gratuitamente e eletronicamente junto à justiça trabalhista (TST);
- III. Prova de regularidade perante a Seguridade Social, mediante a apresentação dos seguintes documentos:
III.I CRF – Certificado de Regularidade do FGTS, emitido pela Caixa Econômica Federal;
- IV. Comprovação do vínculo dos profissionais executantes com a empresa prestadora de serviços, conforme ANEXO II;
- V. É requisito para habilitação da empresa capital social compatível com o número de empregados, observando-se parâmetros estabelecido no Art. 4º-B da Lei 13.429, de 31 de março de 2017 ou capital mínimo ou de patrimônio líquido mínimo, não inferior a 10% (dez por cento) do valor estimado da contratação;
- VI. Documentos do Manual de Terceiro, assinalados no ANEXO III. Excepcionalmente, os documentos relativos ao Manual de Terceiro, assinalados no anexo III, deverão ser apresentados e entregues até o 40º (quadragésimo) dia após a assinatura do Contrato de Prestação de Serviços, sob pena de rescisão.

8.4 Os documentos devem ser enviados juntamente com a proposta, sob pena de eliminação.

8.5 A qualificação exigida deverá ser mantida vigente durante toda vigência do contrato a ser firmado com a empresa ganhadora.

8.6 Se a empresa estiver desobrigada da apresentação de quaisquer documentos solicitados deverá comprovar esta condição por meio de certificado expedido por órgão competente ou legislação em vigor.

8.7 Caso necessário, o responsável pelo presente processo, poderá solicitar visita técnica à empresa que apresentar melhor proposta e documentação obrigatória de acordo com o Termo de Referência, cabendo ao setor de qualidade do hospital realizar a visita técnica no prazo máximo de 5 dias úteis posterior a data da solicitação de visita requerida, apresentando o resultado da avaliação em até 2 dias úteis após a visita técnica.

9. DOS ESCLARECIMENTOS, IMPUGNAÇÕES E RECURSOS:

9.1 Será permitido esclarecimento de dúvidas até o terceiro dia útil após a publicação do Termo de Referência, somente através do e-mail: **compras.tr@hejsn.aebes.org.br**. Na solicitação de esclarecimentos, a empresa deverá apresentar sua razão social, número de CNPJ, identificar o nº do Termo de Referência e objeto da contratação, devendo o questionamento ser redigido de forma clara e objetiva.

9.2 A empresa que solicitar esclarecimentos, deverá informar os contatos para retorno, telefone e e-mails.

9.3 As solicitações de esclarecimentos que não atenderem os requisitos dos itens anteriores, não serão respondidos.

9.4 Serão recebidas as impugnações enviadas até às 17h do quinto dia útil anterior à data limite para o recebimento das propostas.

9.5 Não serão conhecidas às impugnações e os recursos apresentados fora do prazo estabelecido neste Termo de Referência.

9.6 As impugnações e pedidos de esclarecimentos não suspendem os prazos previstos no certame. No entanto, caso o responsável pelo processo julgue pelo acolhimento de eventual impugnação contra o ato convocatório, poderá ser definida e publicada nova data para o envio de propostas.

9.7 Encerrado o processo na plataforma **www.publinexo.com.br/privado/** o resultado será publicado no site **https://www.evangelicovv.com.br/institutional/129-briefings-hejsn**, qualquer participante do referido Termo de Referência poderá recorrer do resultado, interpondo o recurso com as razões de pedido e seus fundamentos, até às 17h do terceiro dia útil, após a data de publicação, de forma motivada e com o registro de suas razões.

9.8 A falta de interposição do recurso contendo suas razões de pedido e seus fundamentos por parte dos participantes, na forma e prazo estabelecidos nos itens anteriores, importará decadência desse direito, ficando o responsável pelo presente processo autorizado a homologar o objeto ao participante declarado vencedor.

9.9 Os recursos deverão ser endereçados ao endereço de e-mail **compras.tr@hejsn.aebes.org.br** e dirigidos ao responsável pelo presente processo. O e-mail deverá conter razão social, número do cartão CNPJ, identificar o nº do Termo de Referência e objeto da contratação e as alegações. Caberá ao responsável pelo presente processo receber, examinar e decidir os recursos impetrados contra suas decisões, no prazo de 06 (seis) dias úteis do recebimento do recurso.

9.10 O acolhimento de recurso importará a invalidação apenas dos atos insuscetíveis de aproveitamento.

9.11 Decididos os recursos e constatada a regularidade dos atos praticados, o responsável competente adjudicará o objeto e homologará o processo de contratação.

10. DISPOSIÇÕES FINAIS

10.1 O presente Termo de Referência não importa necessariamente em contratação, podendo a AEBES revogá-la, no todo ou em parte, por razões de interesse público, derivadas de fato supervenientes comprovados ou anulá-la por ilegalidade, de ofício ou por provocação, mediante ato escrito e fundamentado, disponibilizado no sistema para conhecimento dos interessados. A ASSOCIAÇÃO EVANGÉLICA BENEFICENTE ESPÍRITO SANTENSE – AEBES poderá, ainda, prorrogar, a qualquer tempo, os prazos para recebimento das propostas e divulgação do resultado, bem como corrigir possíveis erros materiais no documento publicado, mediante errata.

10.2 O foro designado para julgamento de quaisquer questões judiciais resultantes deste Termo de Referência será a Comarca de Vitória – ES.

10.3 Aquele que deixar de entregar ou de apresentar documentação exigida no Termo de Referência, apresentar documentação falsa, ensejar o retardamento da execução de seu objeto, não mantiver a proposta, falhar ou fraudar na execução do contrato, comportar-se de modo inidôneo, fizer declaração falsa ou cometer fraude fiscal e que, convocado dentro do prazo de validade de sua proposta, não assinar o contrato, ficará sujeito a reparação dos danos causados ao Hospital.

10.4 É vedada a participação no mesmo Termo de Referência de pessoas jurídicas que sejam controladoras, controladas, coligadas ou integrantes de um mesmo grupo econômico.

(IMPRESSÃO EM PAPEL TIMBRADO DA EMPRESA)
(ANEXO I)

ATESTADO DE CAPACIDADE TÉCNICA

Atestamos, para fins de prova, aptidão de desempenho e atestado de execução, que a empresa **[nome da empresa prestadora de serviços, em negrito]**, inscrita no CNPJ sob o nº 00.000.000/0000-00, estabelecida na Rua, nº....., bairro, na cidade de, Estado de, prestou serviços à **[nome da empresa contratante, em negrito]**, CNPJ nº 00.000.000/0001-00, de **[descrição dos serviços prestados, especificando o prazo de execução]**.

Registramos, ainda, que as prestações dos serviços acima referidos apresentaram bom desempenho operacional, tendo a empresa cumprido fielmente com suas obrigações, nada constando que a desabone técnica e comercialmente, até a presente data.

[cidade/estado], em XX de XXXX de 201X.

Assinatura do responsável legal

[Razão social da empresa]

CNPJ nº xx.xxx.xxx/xxxx-xx

[endereço da empresa, caso não possua papel timbrado]

(IMPRESSÃO EM PAPEL TIMBRADO DA EMPRESA)
(ANEXO II)

DECLARAÇÃO DE VÍNCULO

Declaramos, para os devidos fins, que os profissionais executantes da prestação de serviço objeto deste Termo de referência são sócios, celetistas ou terceirizados. (Indicar o vínculo dos profissionais)

[cidade/estado], em XX de XXXX de 201X.

Assinatura do responsável legal

[Razão social da empresa]

CNPJ nº xx.xxx.xxx/xxxx-xx

[endereço da empresa, caso não possua papel timbrado]



Anexo III

Código: CONT.FR.0100

Data da
Elaboração:
11/07/2019Revisão:
013
15/02/2024

Documentos solicitados no Termo de Referência.

Setor Pessoal

- Ficha de Registro do Ministério do Trabalho e Emprego dos empregados que prestam serviço na AEBES;
- GFIP – Guia de recolhimento de FGTS e Informações à Previdência Social – dos funcionários que prestam serviço na AEBES – para identificarmos o código de recolhimento (Mensal)
- RE – Relação de Empregados; RET (Relação de Tomadores);
- Comprovante declaratório das contribuições a recolher à Previdência Social e outras entidades do Fundo de FPAS da empresa Contratada (Mensal)
- GPS – Guia Previdência Social Atual – para comprovação de pagamento dos impostos exigidos por lei (Mensal)
- Crachá de identificação com nome da instituição, nome do empregado, foto e cargo.
- Outros: _____

Medicina do Trabalho

- PCMSO – Programa de Controle de Médico e Saúde Ocupacional – NR 07, válido conforme período contratual (Anual);
- ASO (Atestado de Saúde Ocupacional) Admissional e Periódico.
- Cópia do Cartão de Vacina contendo as vacinas Tétano e Difteria (DT) e Hepatite B e demais vacinas de campanhas promovidas pelo Ministério da Saúde; (**Triplíce Viral, Influenza e Febre Amarela**);
- Outros: _____

Segurança do Trabalho

- PGR (Programa de Gerenciamento de Riscos – NR 09), válido conforme período contratual (Anual);
- PCMAT (Programa de Condições e Meio Ambiente de Trabalho na Indústria da Construção - NR18), válido conforme período contratual (Anual). Exigido somente para as empresas de construção civil;
- Ficha de Controle de EPI (Equipamento Proteção Individual – NR 06) contendo o CA (Certificado de Aprovação)
- Outros: _____

Treinamento e Desenvolvimento

- Contendo: NR 32 NR 06 CIPA NR 10 NR 33 NR 35 Biossegurança
 ACLS _____ _____ _____

**MINUTA DE CONTRATO
(ANEXO IV)**

CT: 0XX/20XX

**CONTRATO DE PRESTAÇÃO DE SERVIÇOS QUE
ENTRE SI FAZEM A ASSOCIAÇÃO EVANGÉLICA
BENEFICENTE ESPÍRITO SANTENSE E (RAZÃO
SOCIAL DA CONTRATADA).**

CONTRATANTE: ASSOCIAÇÃO EVANGÉLICA BENEFICENTE ESPÍRITO SANTENSE – AEBES, (QUALIFICAÇÃO HEJSN)

CONTRATADA: (RAZÃO SOCIAL, QUALIFICAÇÃO DA EMPRESA, RESPONSÁVEL LEGAL, QUALIFICAÇÃO DO RESPONSÁVEL), ajustam o presente contrato de prestação de serviços, de acordo com as cláusulas seguintes:

CLÁUSULA PRIMEIRA – DO OBJETO CONTRATUAL

1.1 O objeto do presente contrato é a **prestação de serviços de infraestrutura de Rede Wi-Fi, com fornecimento de equipamentos para transmissão do sinal ARUBA**, a ser executado nas dependências do Hospital Estadual Dr. Jayme Santos Neves (HEJSN), sob a gestão da CONTRATANTE.

- a) O serviço abrangerá as atividades de solução de controle de acesso, solução de gerência de hardware, controlador wlan hardware, pontos de acesso interno, ponto de acesso cabeado, conexão entre os pontos, rack, atendimento dos níveis de serviço e manutenção da rede, atuando em conjunto com os profissionais do HEJSN.

1.2 Os serviços, objeto deste instrumento, serão realizados pela CONTRATADA, tendo por executores, profissionais plena e legalmente aptos, capacitados e habilitados.

1.3 A CONTRATADA declara para todos os fins de direito estar devidamente habilitada, consoante a legislação regulamentar, para a prestação do serviço ora contratada.

CLÁUSULA SEGUNDA – DAS OBRIGAÇÕES DA CONTRATADA

2.1 A CONTRATADA deverá:

- a) Iniciar a prestação dos serviços no prazo de até 30 (trinta) dias, a contar da data de início da assinatura do contrato.
- b) Prestar os serviços de forma contínua ao HEJSN, em regime de 24/7.
- c) Prestar suporte e manutenção *on site* durante a vigência do contrato conforme SLA - Service Level Agreement (Acordo de Nível de Serviço - ANS), definido abaixo:

TIPO	INÍCIO DO ATENDIMENTO	PRAZO DE SOLUÇÃO
Serviço parado	2h	Máximo 4h
Sistema com problema ocasionando lentidão	4h	8h
Sistema com problema, mas sem prejudicar operação	12h	48h

- d) Disponibilizar canal de atendimento para abertura de chamados que poderá ser sistema, telefone ou e-mail, com geração de ticket com horário do atendimento e número único para acompanhamento da solução.
- e) Prestar toda configuração e apoio à CONTRATANTE;
- f) Possuir profissional com certificação técnica ACMP (Aruba Certified Mobile Professional), ou seja, na solução do mesmo fabricante do software;
- g) Atender às normas de qualidade e segurança vigentes;
- h) Fornecer produtos mediante solicitação de compra/reposição de estoque em 07 dias;
- i) Fornecer apoio técnico na utilização e manejo dos produtos/equipamento;
- j) Realizar substituição imediata dos equipamentos em casos de manutenções preventivas e corretivas;
- k) Comunicar ao cliente, com a devida antecedência ou de acordo com o nível de serviço qualquer anormalidade na prestação de serviço;
- l) Manter a prestação de serviço sem nenhum tipo de interrupção conforme acordado em contrato.

2.1.1 Não é permitida a subcontratação total ou parcial do objeto deste contrato, bem como sua cessão ou transferência, total ou parcial, pela CONTRATADA;

2.1.2 **O sistema deverá conter:**

I. SOLUÇÃO DE CONTROLE DE ACESSO

- a) Solução ARUBA WIFI com especificações mínimas conforme abaixo:

QUANTIDADE	DESCRIÇÃO
HARDWARE	
39	Aruba IAP-315 (RW) 802.11n/ac Dual 2x2:2/4x4:4 MU-MIMO Radio Integrated Antenna AP
39	PD-9001GR-AC 30W 802.3at PoE+ 10/100/1000 Ethernet Indoor Rated Midspan Injector
39	AP-220-MNT-W1W Flat Surface Wall/Ceiling White AP Basic Flat Surface Mount Kit
39	PC-AC-BR Brazil AC Power Cord
SERVICE	
39	Aruba 3Y FC NBD Exch IAP 315 SVC
SOFTWARE	
39	Aruba Central Device Management 1 Token 3 Year Subscription E-STU
39	Aruba Central Cloud Services 1 Token 3 Year Subscription E-STU

- b)** Solução de autenticação de usuários e dispositivos para controle de acesso à rede baseada em appliance ou software;
- c)** Suportar integração com bases de dados de usuários do tipo LDAP, Active Directory e SQL;
- d)** Implementar gerenciamento e aplicação de políticas de autorização de acesso de usuários com base em:
 - d.1)** Atributos do usuário autenticado;
 - d.2)** Hora do dia, dia da semana;
 - d.3)** Tipo de dispositivo utilizado;
 - d.4)** Localização do usuário;
 - d.5)** Tipo de autenticação utilizado.
- e)** Implementar funcionalidade de classificação automática de dispositivos ("Device profiling"), de forma a descobrir, classificar e agrupar os dispositivos conectados na rede;
- f)** Classificar, no mínimo, por sistema operacional e tipo de dispositivo (Ex. Apple, Samsung);
- g)** Possuir interface para construção de regras e categorias customizadas de classificação de dispositivos;
- h)** Permitir que o administrador cadastre manualmente um determinado dispositivo em uma categoria;
- i)** Possuir base de regras e categorias de dispositivos pré-configurada;
- j)** Suportar mecanismo de atualização das regras e categorias pré-configuradas;
- k)** Implementar os serviços de autenticação, profiling e autorização para no mínimo 170 usuários/dispositivos simultâneos. Caso exista licenciamento distinto para usuários/dispositivos da rede sem fio (wireless) e usuários/dispositivos da rede cabeada (wired), deverão ser fornecidas as duas licenças para o número total de usuários solicitados.
- l)** Possuir recursos integrados de AAA, permitindo que a solução possa ser utilizada como plataforma de autenticação (RADIUS);
- m)** Possuir suporte a TACACS+;
- n)** Possuir CA integrada, para geração de certificados para os dispositivos que forem se autenticar na rede;
- o)** Permitir que a solução faça consultas em bases SQL, com o objetivo de buscar informação a serem utilizadas durante o processo de autenticação dos usuários;
- p)** Possuir ferramenta para gerenciar os processos de credenciamento, autenticação, autorização e contabilidade de usuários visitantes através de um portal web seguro;
- q)** Suportar dispositivos visitantes conectados simultaneamente na rede via portal web;
- r)** Implementar a criação de grupos de autorizadores com privilégios distintos, por SSID, de criação de credenciais temporárias e atribuição de permissões de acesso aos clientes;

- s) Realizar a autenticação dos autorizadores em base externa do tipo Microsoft Active Directory ou LDAP e atribuir o privilégio ao autorizador de acordo com o seu perfil;
- t) Implementar as funcionalidades de geração aleatória de lotes de credenciais temporárias pré-autorizadas;
- u) Implementar a importação e exportação da relação de credenciais temporárias através de arquivos.txt ou csv;
- v) Permitir a criação de validade das credenciais, baseando o início da validade na criação da conta ou no primeiro login da conta;
- w) Permitir que o visitante crie sua própria credencial temporária ("self-service") através do portal web, sem a necessidade de um autorizador;
- x) Permitir a customização do formulário de criação de credenciais, a ser preenchido pelo autorizador ou pelo visitante, em caso de autosserviço, especificando quais informações cadastrais dos visitantes são obrigatórias ou opcionais;
- y) Permitir a customização do nível de segurança da senha temporária que será gerada ao visitante, especificando a quantidade mínima de caracteres e o uso de caracteres especiais e números para compor a senha;
- z) Exigir que o usuário visitante aceite o "Termo de uso da rede" a cada login ou apenas no primeiro login;
- aa) Permitir o envio das credenciais aos usuários registrados através de mensagens SMS (Short Message Service), e-mail e impressão local;
- bb) Todas as licenças deverão ser permanentes e perpétuas. Não serão aceitos licenciamento de recursos com prazos limitados de utilização;
- cc) Suportar em caso de necessidade futura controle de acesso à rede cabeada;
- dd) Possuir a possibilidade de configuração de VLAN de pré-autenticação onde os usuários se conectam a uma VLAN ao ligar a máquina e após efetuar o login a VLAN seja alterada de acordo com a política aplicada ao login do usuário;
- ee) O Hardware necessário para funcionamento do software de controle de acesso será fornecido pela empresa contratada, podendo ser servidor, uma máquina virtual, appliance ou em cloud, deverá possuir capacidade de hardware suficiente para executar todas as funcionalidades do projeto, deverá possuir fontes de alimentação e discos rígidos redundantes, deverá possuir suporte com tempo de solução de problemas de até 6 horas. Deverá fornecer as licenças de sistema operacional, caso seja necessário. Podendo optar por solução free.

II. SOLUÇÃO DE GERÊNCIA DE HARDWARE

- a) A Solução de Gerência da Rede Sem Fio deve ser fornecida como serviço;

- b)** Caso exista a possibilidade de fornecimento em Appliance Virtual, deve ser fornecido o servidor com a capacidade recomendada pelo fabricante, comprovada por documento oficial com todas as licenças incluídas, inclusive de sistema operacional e outras que sejam necessárias para o funcionamento do sistema;
- c)** Ser obrigatoriamente do mesmo fabricante dos pontos de acesso e controladores;
- d)** Permitir a configuração e gerenciamento através de browser padrão seguro HTTPS;
- e)** Ser capaz de gerenciar todos os APs e controladores WLAN;
- f)** Permitir que os eventos sejam gravados remotamente utilizando Syslog;
- g)** Prover organização hierárquica de equipamentos, permitindo que um equipamento receba as configurações lógicas e as replique a outros equipamentos;
- h)** Possuir capacidade de projeto automatizado de redes sem fio nos padrões 802.11a, 802.11b e 802.11g, 802.11n e 802.11ac, segundo a geografia do prédio (planta);
- i)** Considerar a área de cobertura e a banda por usuário desejada;
- j)** Possibilitar a importação de plantas baixas nos formatos .dwg e .jpg;
- k)** Permitir a visualização de alertas da rede em tempo real;
- l)** Permitir a visualização de eventuais áreas sem cobertura de RF (áreas de sombra);
- m)** Monitorar o desempenho da rede wireless, consolidando informações de rede tais como: níveis de ruído, relação sinal-ruído, interferência, potência desinal;
- n)** Possuir capacidade de listagem on-line da localização de usuário, endereço IP, endereço MAC, nível de potência de recepção e dados de associação e de autenticação 802.1x;
- o)** Possuir informação visual e gráfica, planta baixa dos andares, para:
 - o.1)** Visualização dos APs instalados, com estado de funcionamento;
 - o.2)** Visualização do mapa de calor de RF(Heatmap);
 - o.3)** Localização de ativos conectados à rede (equipamentos 802.11);
 - o.4)** Localização de rogue APs.
- p)** Caso esta funcionalidade não esteja disponível no sistema de gerência, deve ser fornecido software, do mesmo fabricante, para atender este item, contemplando toda a rede e com redundância 1+1.
- q)** Possuir capacidade de identificação e listagem dos rádios vizinhos e respectivos SSID/BSSID que podem ser percebidos por cada AP;
- r)** Possuir capacidade de configuração gráfica completa do Controlador WLAN e respectivos APs;

- s)** Possuir capacidade de geração de relatórios dos seguintes tipos:
 - s.1)** Visualização dos APs instalados, com estado de funcionamento;
 - s.1)** Listagem de clientes Wireless;
 - s.1)** Listagem de APs;
 - s.1)** Informações de Configuração dos Controladores WLAN;
 - s.1)** Utilização da rede;
 - s.1)** Detalhes dos APs não autorizados (rogues) detectados.

- t)** Suportar SSH, HTTP/HTTPS, SSL, Telnet;

- u)** Possuir ferramentas de debug e log de eventos para depuração e gerenciamento em primeiro nível;

- v)** Implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps;

- w)** Possuir suporte a MIB II, conforme RFC1213;

- x)** Implementar a MIB privativa que forneça informações relativas ao funcionamento do equipamento;

- y)** Possibilitar a obtenção da configuração do equipamento através do protocolo SNMP;

- z)** Possibilitar a obtenção via SNMP de informações de capacidade e desempenho da CPU, memória e portas;

- aa)** Possibilitar a gerência e identificação individualizada de cada AP remoto;

- bb)** Permitir a administração centralizada dos APs sem a necessidade de configurar os APs individualmente;

- cc)** Possibilitar a identificação de paredes e divisórias com respectivos níveis de atenuação por tipo (alvenaria, vidro, drywall e divisória);

- dd)** Possibilitar a importação de plantas baixas nos formatos gráficos (CAD, .dwg, .jpg, .gif e .png);

- ee)** Disponibilizar em painel gráfico de controle informações referentes à:
 - ee.1)** Visualização dos APs instalados, com estado de funcionamento;
 - ee.2)** Sistemas operacionais e tipos de dispositivos que estão se conectando a rede;
 - ee.3)** Informações sobre chamadas de voz, seus protocolos e qualidade delas;
 - ee.4)** Informações sobre os tipos de aplicações mais utilizados;
 - ee.5)** Informações sobre usuários conectados.

- ff)** Possuir informação sobre possíveis ameaças a rede detectadas pelos sistemas gerenciados;

- gg)** Possibilitar criação de regras de detecção de ameaças e correlacionar todos os dispositivos gerenciados.

III. CONTROLADOR WLAN HARDWARE

- a)** Solução baseada em hardware, virtual ou cloud o, do mesmo fabricante dos pontos de acesso e software de gerência;

- b) Não serão aceitos hardwares genéricos.
- c) Gerenciar, no mínimo, a quantidade de 40 pontos de acesso simultaneamente, com centralização das funcionalidades de autenticação;
- d) Permitir a conexão simultânea de, no mínimo, 2.000 clientes wireless;
- e) Permitir o armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior à queda de alimentação;
- f) Permitir gravação de múltiplas configurações no próprio equipamento;
- g) Possuir fonte de alimentação com seleção automática de tensão (100-240VAC);
- h) Permitir a gravação de eventos por meio do protocolo Syslog;
- i) Possuir capacidade de gerenciamento hierárquico, com possibilidade de definição de grupos de equipamentos e alteração das características de configuração do grupo sem a necessidade de configuração individual de cada equipamento;
- j) Acesso ao sistema através de cliente com browser padrão (HTTP, HTTPS, Java);
- k) Possuir LEDs para a indicação do status das portas e atividade;
- l) Permitir ser montado em rack padrão de 19 (dezenove) polegadas, incluindo todos os acessórios necessários;
- m) Ser acompanhado de todos os acessórios necessários para operacionalização do equipamento, tais como: softwares, cabos de console, cabos de energia elétrica, documentação técnica e manuais que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização do equipamento;
 - m.1) Caso a controladora não possua as interfaces de rede solicitadas, poderá ser ofertado um switch LAN com as características de portas de rede solicitadas, para cada controladora ofertada.
- n) Permitir operação em modo mesh;
- o) Permitir o uso de múltiplos SSIDs simultaneamente;
- p) Prover tempo de fast-roaming intra-switch inferior a 25milissegundos;
- q) Permitir conexão entre APs sem a necessidade de conexão cabeada, implementando assim uma rede padrão mesh;
- r) Prover tempo de fast-roaming inter-switch em camada 2 inferiores a 100 milissegundos;
- s) Suportar 802.11e com WMM, U-APSD eT-SPEC;

- t) Gerenciar centralizadamente a autenticação de usuários;
- u) Implementar protocolo de autenticação para controle do acesso administrativo ao equipamento com mecanismos de AAA;
- v) Possuir base de dados de usuários interna para autenticação de usuários convidados/temporários (acesso guest);
- w) Permitir autenticação em no mínimo os seguintes sistemas de base de dados de usuários Microsoft Active Diretor, Cisco ACS server, Free Radius, entre outros;
- x) Realizar o provisionamento de usuários convidados (guests) através de interface Web por meio de um usuário administrativo com permissões mínimas, exclusivas para este fim;
- y) Possuir suporte a autenticação IEEE 802.1X, com pelo menos os seguintes métodos EAP: EAP-MD5, PEAP/EAP- GTC, PEAP/EAP-MSCHAPv2, EAP-TLS com utilização de base de usuários interna ou servidor RADIUS externo;
- z) Suportar as especificações abaixo:
 - z.1) RFC2409;
 - z.2) RFC2661;
 - z.3) RFC2408;
 - z.4) RFC3602;
 - z.5) RFC3948;
 - z.6) RFC2548.
- aa) Suportar os seguintes métodos:
 - aa.1) RFC2409;
 - aa.2) EAP-PEAP
 - aa.3) EAP-TLS
 - aa.4) EAP-TTLS;
- bb) Possuir suporte a autenticação IEEE 802.1X, com o método PEAP/EAP-GTC, e com utilização de base de usuários LDAP externa;
- cc) Permitir a seleção / uso de servidor Radius ou LDAP com base no SSID;
- dd) Suportar a autenticação de usuários conectados à rede cabeada através das portas do controlador;
- ee) Possuir o recurso de EAP Offload para terminação do túnel EAP no próprio controlador;
- ff) Suportar utilização de Portal Captivo externo ao controlador;
- gg) Permitir a autenticação (através de endereço MAC, Portal Captivo ou IEEE 802.1X) de usuários conectados à rede WLAN (wireless) ou usuários conectados às portas cabeadas do controlador. Também deverá permitir a autenticação de usuário e de máquina por meio de IEEE802.1x;

- hh)** Oferecer recurso de Portal Captivo (Captive Portal) com suporte a múltiplos portais simultaneamente;
- ii)** Implementar associação dinâmica de usuário a VLAN, com base nos parâmetros da etapa de autenticação;
- jj)** Implementar Qualidade de Serviço com a marcação de pacotes utilizando Diffserv e suporte a 802.1p para QoS de rede;
- kk)** Possibilitar roaming com integridade de sessão, dando suporte a aplicações em tempo real, tais como, VoIP, VoWLAN, videoconferência, dentre outras;
- ll)** Permitir portais captivos externos a controladora;
- mm)** A controladora deve possuir funcionalidade de conexão Site to Site VPN utilizando padrão Ipsec.
- nn)** Caso a solução fornecida não possua a funcionalidade, será aceita solução de VPN adicional;
- oo)** Implementar segurança IEEE802.11i;
- pp)** Suportar a criptografia centralizada com os seguintes protocolos: AES-CCMP, TKIP e WEP;
- qq)** Suportar, no mínimo, 2000 VLANs;
- rr)** Implementar o protocolo 802.1w (Rapid Spanning Tree);
- ss)** Oferecer suporte a roteamento e switching de camadas L2 e L3;
- tt)** Suportar as especificações abaixo:
 - tt.1)** RFC 2328;
 - tt.2)** RFC2338;
 - tt.3)** RFC1027;
 - tt.4)** IEEE 802.1w;
 - tt.5)** RFC 1519.
- uu)** Possuir o recurso de criação de Pools de VLAN para permitir a escalabilidade de redes;
- vv)** Possuir servidor DHCP embutido;
- ww)** Suportar o protocolo VRRP para redundância de controladores;
- xx)** Suportar redundância de controladores conectados em camada 3;
- yy)** Suportar redundância de controladores nos modos:
 - yy.1)** 1+1;
 - yy.1)** N+1;
 - yy.1)** Ativo-Ativo;
 - yy.1)** Ativo-Standby.

- zz)** Oferecer os recursos de mobilidade entre VLANs para roaming de camada 2;
- aaa)** Oferecer os recursos de Proxy de endereços IP e Proxy DHCP para roaming entre redes (L3);
- bbb)** Implementar tagging de VLANs através do protocolo 802.1Q;
- ccc)** Implementar o protocolo 802.1d para Spanning Tree (STP);
- ddd)** O controlador WLAN poderá estar diretamente e/ou remotamente conectado aos APs por ele gerenciados, inclusive via roteamento nível 3 da camada OSI;
- eee)** Se um controlador WLAN falhar, os APs relacionados deverão se associar a um controlador WLAN alternativo de forma automática, não permitindo que a rede wireless se torne inoperante;
- fff)** Realizar a descoberta automática dos APs na infraestrutura wireless;
- ggg)** Permitir o controle dos APs mediante a conexão através de topologia MESH (WiFiMesh);
- hhh)** A rede MESH deverá oferecer comportamento determinístico da topologia da rede MESH;
- iii)** A rede MESH deverá prover auto-redundância das camadas física (RF) e Layer 2 com comportamento determinístico;
- jjj)** Permitir a conexão de APs de maneira remota e segura;
- kkk)** Conectar APs através de redes públicas e/ou privadas com garantia de segurança através de conexão criptografada;
- lll)** Permitir a propagação de SSIDs de maneira segura para qualquer AP legitimamente cadastrado na controladora, independentemente de onde este AP esteja conectado;
- mmm)** Permitir a autenticação do AP remoto através de certificado digital ou de usuário e senha cadastrados em servidor AD e Radius;
- nnn)** Gerenciar o tráfego dos APs centralizadamente;
- ooo)** Permitir o uso de, pelo menos, uma interface Ethernet com rede segmentada para gerenciamento;
- ppp)** Otimizar o desempenho e a cobertura da radiofrequência;
- qqq)** Ajustar automaticamente os canais de modo a otimizar a cobertura de rede e mudar as condições de RF baseado em performance;
- rrr)** Detectar interferência e ajustar parâmetros de RF, evitando problemas de cobertura e controle da propagação indesejada de RF;
- sss)** Implementar varredura de RF contínua, programada ou sob demanda, com identificação de APs ou clientes irregulares;

- ttt)** Implementar a tecnologia de "Channel load balancing", permitindo que clientes sejam automaticamente distribuídos entre Pontos de Acesso adjacentes operando em canais distintos, com o objetivo de balancear a carga entre os Pontos de Acesso;
- uuu)** Implementar a tecnologia de "Band Steering/Select", permitindo que clientes com suporte a faixa de frequência de 5GHz se conectem aos Pontos de Acesso utilizando, preferencialmente, a faixa de 5GHz;
- vvv)** Implementar varredura de RF nas bandas 802.11a, 802.11b, 802.11g, 802.11n e 802.11ac para identificação de ataques e APs intrusos não autorizados (rogues);
- www)** Realizar a varredura no canal de operação do AP sem impacto na performance da rede WLAN;
- xxx)** Permitir a varredura em todos os canais possíveis de RF para detecção e contenção de ameaças na rede WLAN;
- yyy)** Fazer a varredura dos espectros de 2,4 GHz e 5 GHz para localização e classificação de interferências não 802.11, análise de espectro, e evitá-las automaticamente;
- zzz)** Detectar áreas de sombra de cobertura e efetuar os devidos ajustes para sua correção, automaticamente;
- aaaa)** Ajustar, dinamicamente, o nível de potência e canal de rádio dos APs, de modo a otimizar o tamanho da célula de RF, garantindo a performance e escalabilidade;
- bbbb)** Permitir o controle de banda disponível (bandwidth contracts) por usuário ou através de perfis de usuários;
- cccc)** Possibilitar roaming com integridade de sessão, dando suporte a aplicações em tempo real, tais como, VoIP, VoWLAN, videoconferência, dentre outras;
- dddd)** Possuir mecanismo de controle de admissão de chamadas nos pontos de acesso (CAC);
- eeee)** A controlador de possuir funcionalidade de conexão Site to Site VPN utilizando padrão Ipsec. Caso a solução fornecida não possua a funcionalidade, será aceita solução de VPN adicional;
- ffff)** Possuir mecanismo automático de QoS para protocolos de voz (SIP, SVP e SCCP) utilizando inspeção automática de pacotes, sem a necessidade de fazer a marcação prévia (tagging) de pacotes;
- gggg)** Possuir solução de identificação de aplicações através de técnicas de análise de tráfego, provendo informações das aplicações mais utilizadas na interface gráfica;
- hhhh)** Permitir a criação de políticas de acesso baseadas nas aplicações, como por exemplo, o acesso a "redes sociais" terá um controle de banda de 2Mbps.
- iiii)** Apresentar informações gráficas referente a utilização de soluções de comunicações unificadas (UC) sobre a infraestrutura WLAN, de formar a apresentar informações referentes as chamadas realizadas e relações gráficas entre o nível de sinal recebido pelo usuário e a qualidade da chamada.

- jjjj) Possuir a funcionalidade da utilização do protocolo Bonjour na infraestrutura, permitindo que os serviços divulgados via mDNS sejam controlados, filtrados e disponibilizados entre diferentes subnets, tornando assim possível a utilização em redes com múltiplas subnets e um número grande de dispositivos.

IV. SERVIÇOS DE INFRAESTRUTURA

- a) Todos os equipamentos de distribuição de sinal WIFI deverão ser interligados com cabo UTP cat. 6 com todas as conexões com conectores cat.6.
- b) A estrutura deverá toda ser organizada em patch panel cat6.
- c) Todos os pontos e equipamento deverão ser identificados com etiquetas com nomenclatura definida pela equipe de T.I. do HEJSN.
- c.1) Instalação de toda infraestrutura;
 - c.2) Lançamento de cabos UTP Cat 6;
 - c.3) Conectorização de cabos UTP Cat 6;
 - c.4) Lançamento de cabos elétricos;
 - c.5) Montagem de tomadas;
 - c.6) Identificação e testes;
 - c.7) ART;
 - c.8) Instalação de todos os pontos de acesso WIFI;
 - c.9) Instalação de pontos de rede;
 - c.10) Treinamento para a equipe de T.I. do HEJSN. Ele deverá abranger toda configuração e manutenção da solução, com no mínimo 10 horas de duração para no mínimo 4 funcionários.

V. QUANTIDADE:

LOCAL	QTD	COBERTURA
1 ANDAR - D	1	CENTRO DE ENSINO E PESQUISA
1 ANDAR - E	1	SALA DE TREINAMENTO
1 ANDAR - F	3	CTQ / UTQ
2 ANDAR - F	5	ACTI ADULTO
3 ANDAR - F	6	UTIN, UCIN, CO
4 ANDAR - F	4	MATERNIDADE
5 ANDAR - F	3	INTERNAÇÃO
6 ANDAR - F	4	INTERNAÇÃO
TERREO - C	1	CENTRO CIRURGICO
TERREO - D	5	PRONTO SOCORRO
TERREO - F	6	IMAGEM, AMBULATORIO, USI
TOTAL:	39	

2.2 A CONTRATADA executará as atividades com autonomia, cabendo a CONTRATANTE a fiscalização do cumprimento do contrato, de forma assegurar a execução do contrato.

2.3 A CONTRATADA se obriga pelo sigilo das informações e nem poderá tornar-se de conhecimento de terceiros, por constituir falta grave e falta de ética dos serviços prestados por parte da CONTRATADA.

2.4 Fornecer à CONTRATANTE todas as informações necessárias à plena execução do serviço contratado.

2.5 Realizar os serviços conforme preceitua o objeto deste contrato, nos locais e condições que melhor atenderem às necessidades e conveniências da CONTRATANTE.

2.6 Requerer a exclusão da CONTRATANTE, individual ou coletivamente, no polo passivo dos eventuais processos judiciais ou administrativos em que a CONTRATADA deu causa, na ocorrência de ação contra a CONTRATANTE, ou qualquer outro ato de natureza administrativa ou judicial, que venha a ser proposto contra a CONTRATANTE, seja a que título for e a que tempo ocorrer, em virtude do presente contrato. A CONTRATADA concorda ainda, desde já, que a CONTRATANTE denuncie à lide ou chame ao processo, se necessário, a CONTRATADA, na forma do artigo 125 do Código de Processo Civil.

2.7 Responsabilizar-se por todos os riscos e despesas decorrentes da contratação de funcionários utilizados na execução do presente contrato, bem como se responsabilizando quanto ao comportamento e eficiência deles, devendo a CONTRATADA substituir em 24 (vinte e quatro) horas, o profissional que não atender às necessidades descritas neste contrato e seus respectivos aditivos e anexos e/ou que não atenda aos princípios da ética, bem como das normas vigentes da Instituição, afastando-o de forma imediata de todas as unidades geridas pela AEBES.

2.8 Não admitir e nem aliciar qualquer empregado que esteja à disposição da CONTRATANTE ou que integre o seu quadro de pessoal.

2.9 Manter, durante a execução do contrato, em compatibilidade com as obrigações assumidas pela CONTRATADA, todas as condições de qualificação, habilitação técnica, jurídica, bem como de regularidade fiscal e trabalhista, exigidas no momento da assinatura deste contrato.

2.10 Manter em condições legais as contribuições trabalhistas e previdenciárias do(s) profissional (s) recrutado(s) para executar os serviços objeto deste contrato.

2.11 A CONTRATADA se obriga em prestar os serviços, objeto deste contrato, observando prazo, qualidade e zelo dos serviços.

2.12 Assumir integralmente a responsabilidade por danos causados à CONTRATANTE ou a terceiros, decorrentes de negligência, imprudência ou imperícia na execução dos serviços contratados.

2.13 Cumprir integralmente todas as obrigações relativas à Segurança do Trabalho utilizando dos equipamentos de proteção individual (EPI'S) necessários à execução dos serviços objeto deste contrato, apresentando os documentos, conforme portaria 3.214/78 do Ministério do Trabalho, a Consolidação das Leis do Trabalho e demais órgãos fiscalizadores.

2.14 Fornecer sempre que forem solicitados, mantendo atualizado junto a CONTRATANTE, os seguintes documentos: cópia do Contrato Social e suas alterações, certidões de regularidade e responsabilidade técnica de conselho regulador, caso tenha, e eventuais alvarás inerentes as atividades prestadas.

2.15 Em caso de descumprimento das obrigações, a CONTRATANTE se reserva no direito de emitir notificação de descumprimento contratual à CONTRATADA, e, em havendo reincidência, caberá imposição de multa, progressivamente até o limite de 10% (dez por cento) do valor do contrato.

CLÁUSULA TERCEIRA – DAS OBRIGAÇÕES DA CONTRATANTE

3.1 Estando o objeto do presente contrato de prestação de serviços, diretamente vinculado e relacionado ao Contrato de Gestão e Operacionalização do Hospital Estadual Dr. Jayme Santos Neves, firmado entre a CONTRATANTE e a SECRETARIA ESTADUAL DE SAÚDE DO ESTADO DO ESPÍRITO SANTO, obriga-se a CONTRATANTE a efetuar o pagamento do valor devido à CONTRATADA, conforme cláusula de pagamento, contados do efetivo recebimento dos recursos financeiros, quer oriundo do Estado ou da União. Para tanto, observada a necessidade prévia da emissão de Nota Fiscal de Serviços pela CONTRATADA, que não poderá em nenhuma hipótese efetuar faturamento direto de quaisquer procedimentos a outro CONTRATANTE ou tomador eventual de serviços, incluindo o poder público, sendo esta prerrogativa exclusiva da CONTRATANTE no âmbito do Hospital Estadual Dr. Jayme Santos Neves, neste Estado do Espírito Santo.

3.2 Fornecer e permitir acesso a todas as informações pertinentes e necessárias ao bom andamento dos serviços a serem desenvolvidos pela CONTRATADA, assim como quaisquer outras informações que tão somente digam respeito às atividades da CONTRATADA.

3.3 Fiscalizar o presente contrato, cabendo verificar se as obrigações assumidas contratualmente estão sendo cumpridas.

3.4 Notificar a CONTRATADA em caso de descumprimento das suas obrigações contratuais.

3.5 A CONTRATANTE deverá facilitar o acesso da CONTRATADA para a consecução do objeto deste contrato;

CLÁUSULA QUARTA – DA REMUNERAÇÃO

4.1 A CONTRATANTE pagará à CONTRATADA, (descrever valor), conforme proposta comercial.

4.2 Por ocasião dos pagamentos serão efetuados os descontos legais por tributos que incidam ou venham a incidir sobre a prestação do serviço contratado e efetivamente executado.

4.3 O pagamento será efetuado, entre o 1º dia e 10º útil do mês seguinte ao início da prestação de serviço, sendo pagamento mensal 15 dias após o envio da nota fiscal e com os documentos legais atualizados e anexados (Conforme cláusula contratual).

4.4 É expressamente vedado a qualquer das partes desconto ou cobrança de duplicata através de rede bancária ou de terceiros, bem como a cessão de crédito dos valores objetos deste contrato ou sua dação em garantia.

4.5 Os reajustes contratuais serão negociados entre as partes, estando eventual concessão, limitado ao prévio reajuste autorizado pela Secretaria de Saúde do Espírito Santo.

CLÁUSULA QUINTA – DO PRAZO CONTRATUAL

5.1 O prazo de vigência do presente contrato será por até 30 de novembro de 2028, a contar da data de assinatura deste instrumento, ressalvando os casos de rescisão previstos na cláusula sexta.

5.2 Qualquer alteração contratual deverá ser feita mediante termo aditivo.

CLÁUSULA SEXTA – DA RESCISÃO CONTRATUAL

6.1 O presente contrato poderá ser rescindido por acordo entre as partes, mediante celebração de “Distrato” ou unilateralmente, de forma imotivada, pela CONTRATANTE, concedendo-se, à CONTRATADA, aviso prévio de 30 (trinta) dias sendo que, nesta hipótese, não será devido qualquer tipo de multa, à parte que solicitar a rescisão.

6.2 Havendo rescisão do contrato pela CONTRATANTE, e havendo cumprimento de aviso prévio, a CONTRATADA deverá deixar de efetuar a prestação de serviço no último dia de vigência do aviso prévio, sob pena de multa diária equivalente a 10% do valor do contrato.

6.3 A CONTRATADA poderá rescindir o contrato unilateralmente, de forma imotivada, concedendo-se à CONTRATANTE, aviso prévio de 60 (sessenta) dias, de modo a evitar a desassistência e, conseqüentemente, assegurar o interesse público, sob pena de multa diária equivalente a 10% do valor do contrato.

6.4 O presente contrato poderá, ainda, ser rescindido unilateralmente, por qualquer uma das partes, sem concessão de aviso prévio na ocorrência de uma das seguintes situações:

- a) Justo Motivo, decorrente de condutas que levem a quebra de confiança;
- b) Falência, recuperação judicial, e insolvência de qualquer uma das partes.
- c) Descumprimento de qualquer cláusula ou condição estabelecida neste contrato;
- d) Negligência, imprudência, imperícia, incapacidade, dolo ou má-fé por parte da CONTRATADA ou dos profissionais no desempenho dos serviços contratados.

6.5 Este contrato será imediatamente rescindido no caso de encerramento do Contrato de Gestão do Hospital Estadual Dr. Jayme Santos Neves, hipótese em que a AEBES não poderá ser responsabilizada ao pagamento de indenizações ou multas de qualquer natureza.

CLÁUSULA SÉTIMA – DA LEI ANTICORRUPÇÃO

7.1 A CONTRATADA declara conhecer as normas de prevenção à corrupção prevista na legislação brasileira, a Lei nº 12.846/2013 e seus regulamentos e se compromete a cumpri-las fielmente, por si e por seus sócios, administradores e colaboradores. Ainda, se obrigada a CONTRATADA, no exercício dos direitos e obrigações previstos neste Contrato e no cumprimento de qualquer uma de suas disposições: **(i)** não dar, oferecer ou prometer qualquer bem de valor ou vantagem de qualquer natureza a agentes públicos ou a pessoas a eles relacionadas ou ainda quaisquer outras pessoas, empresas e/ou entidades privadas, com o objetivo de obter vantagem indevida, influenciar ato ou decisão ou direcionar negócios ilícitamente e **(ii)** adotar as melhores práticas de monitoramento e verificação do cumprimento das leis anticorrupção, com o objetivo de prevenir atos de corrupção, fraude, práticas ilícitas ou lavagem de dinheiro por seus sócios, administradores, colaboradores e/ou terceiros por elas contratados. A comprovada violação de qualquer das obrigações previstas nesta cláusula é causa para a rescisão unilateral deste Contrato, sem prejuízo da cobrança das perdas e danos causados à parte inocente.

CLÁUSULA OITAVA – DO CÓDIGO DE CONDUTA

8.1 A CONTRATADA se obriga a adotar conduta justa e ética, respeitando as diretrizes estabelecidas no Código de Conduta da CONTRATANTE, disponível no endereço eletrônico <https://www.evangelicovv.com.br/aebes/codigo-conduta>, o qual desde já declara conhecer e estar vinculada.

8.2 A CONTRATADA se compromete, ainda, a treinar seus Colaboradores alocados na execução das atividades deste Contrato, a fim de instruí-los sobre o cumprimento obrigatório das diretrizes contidas no Código de Conduta da CONTRATANTE para a execução do objeto deste instrumento.

CLÁUSULA NONA – DA PROTEÇÃO DE DADOS PESSOAIS NA RELAÇÃO CONTROLADOR E OPERADOR

9.1 Para fins deste contrato, são considerados:

I. “DADOS PESSOAIS”: qualquer informação relativa a uma pessoa natural (TITULAR DE DADOS) que é capaz de identificá-la de forma direta ou indireta, como por exemplo um nome, número de CPF e RG, endereço residencial, dados de localização, ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social de uma pessoa.

II. “DADOS PESSOAIS SENSÍVEIS”: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

III. “TRATAMENTO”: qualquer operação ou conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

IV. “CONTROLADOR”: parte que determina as finalidades e os meios de tratamento de dados pessoais.

V. “OPERADOR”: parte que trata dados pessoais de acordo com as instruções do CONTROLADOR.

VI. “AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS”: Órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional.

9.2 DEFINIÇÃO DAS FUNÇÕES

Esta cláusula aplica-se ao tratamento de dados pessoais, dentro do âmbito da Lei Geral de Proteção de Dados Pessoais - LGPD, pelo OPERADOR em nome do CONTROLADOR.

Para os propósitos deste contrato, as partes supra qualificadas, concordam que a AEBES é o CONTROLADOR dos dados pessoais e a CONTRATADA é o OPERADOR de tais dados, dentro da relação negocial entre as partes.

As PARTES declaram ter conhecimento da Lei 13.709/2018 ("Lei Geral de Proteção de Dados Pessoais - LGPD") e das demais legislações vigentes sobre Proteção de dados pessoais, e se comprometem a cumprir com todas as obrigações legais e contratuais relacionadas às Operações de Tratamento de Dados Pessoais e à proteção, sigilo e privacidade de Dados Pessoais, adotando as medidas técnicas e administrativas cabíveis visando sua conformidade com a privacidade, exigindo de seus colaboradores; prestadores de serviços e fornecedores o mesmo nível aceitável de segurança da informação e confidencialidade, com base nas melhores práticas de mercado.

9.3 OBRIGAÇÕES DO CONTROLADOR

O CONTROLADOR deve:

Implementar medidas técnicas e organizacionais apropriadas para assegurar e demonstrar que o tratamento é realizado de acordo com a LGPD. Essas medidas devem ser revistas e atualizadas sempre que necessário.

Implementar medidas técnicas e organizacionais apropriadas para garantir que, somente os dados pessoais necessários para cada propósito específico sejam tratados. Essa obrigação se aplica à quantidade de dados pessoais coletados, à extensão do tratamento, ao período de armazenamento e à acessibilidade, sempre observando os princípios e fundamentos da LGPD.

Orientar ao OPERADOR, quanto às medidas e limites para o tratamento de dados pessoais, a fim de garantir que o tratamento seja realizado dentro dos padrões técnicos e legais, garantindo a proteção dos dados pessoais tratados pelas partes.

9.4 OBRIGAÇÕES DO OPERADOR

O OPERADOR deve:

Tratar os dados pessoais somente de acordo com as instruções documentadas do CONTROLADOR.

Tratar apenas os dados pessoais e dados pessoais sensíveis estritamente necessárias para atendimento da finalidade/objeto expressamente previsto neste contrato e em observância das regras específicas previstas na Lei nº 13.709/1918 (“LGPD”).

É vedado ao OPERADOR a realização de imagens dos pacientes sem seu respectivo consentimento, sob pena de rescisão do presente instrumento contratual, bem como ressarcimento de todo e qualquer eventual prejuízo sofrido pelo CONTROLADOR, incluindo multas, condenações judiciais, honorários advocatícios e demais penalidades pecuniárias previstas pela legislação vigente.

Manter o sigilo absoluto de todas as informações e dados pessoais a que tenham acesso e garantir que as pessoas autorizadas para o tratamento dos dados pessoais estejam comprometidas com a confidencialidade, em razão da função ou estão sob obrigação contratual.

Adotar todas as ações necessárias para implementar medidas técnicas e organizacionais apropriadas para assegurar um nível de segurança adequado ao risco aos direitos e liberdades das pessoas.

Respeitar as condições de contratação de terceiros, sendo que o OPERADOR não pode contratar outro OPERADOR (Sub Operador) para processamento de dados sem a prévia autorização do CONTROLADOR.

Em caso de requisição de titulares, fica à cargo do CONTROLADOR responder ao titular de dados pessoais, devendo o OPERADOR (i) se abster de responder diretamente ao titular; (ii) notificar ao CONTROLADOR, imediatamente, caso requisitada; e (iii) cooperar e fornecer todas as informações necessárias para a efetivação dos direitos do titular.

Auxiliar o CONTROLADOR a garantir o cumprimento das obrigações relacionadas à segurança do tratamento, Violações de dados pessoais, avaliações de impacto de proteção de dados e plano de resposta à incidentes;

Informar o CONTROLADOR imediatamente, a ocorrência de incidente de segurança relativo ao tratamento de dados pessoais que possa acarretar risco ou dano relevante a esses titulares;

Indenizar o CONTROLADOR por quaisquer perdas e danos devidamente apurados e comprovados (incluindo multas, custos ou despesas e desembolsos legais) incorridos pelo OPERADOR em decorrência de qualquer violação de Dados Pessoais, nos termos da LGPD, por ato ou omissão em conexão com a execução deste Contrato.

Excluir ou devolver todos os dados pessoais ao CONTROLADOR após o término da prestação dos serviços relacionados ao tratamento, e excluir as cópias existentes, a menos que a lei aplicável exija o armazenamento destes dados.

Disponibilizar ao CONTROLADOR todas as informações imprescindíveis para demonstrar o cumprimento das obrigações estabelecidas na LGPD, sempre que necessário.

9.5 VIGÊNCIA DO CONTRATO E LEGISLAÇÃO APLICÁVEL

Este Contrato continuará em vigor enquanto o OPERADOR estiver tratando dados pessoais em nome do CONTROLADOR e será regido pela LGPD e demais legislações de proteção de dados pessoais e privacidade, bem como as normas aplicáveis ao negócio das partes.

CLÁUSULA DÉCIMA – DAS DISPOSIÇÕES GERAIS

10.1 O presente contrato é documento único que regula os direitos e obrigações entre as partes com relação aos serviços contratados, ficando cancelado qualquer outro acordo porventura existente.

10.2 É vedada a transferência deste contrato para terceiros sem a anuência expressa da CONTRATANTE.

10.3 A CONTRATADA obriga-se a comunicar à CONTRATANTE, por escrito, qualquer alteração que pretenda fazer em seu quadro funcional ou societário que implique substituição de membro(s) da equipe que efetivamente realize a prestadora dos serviços objeto do contrato.

10.4 Caso a CONTRATANTE venha a ser acionada judicialmente em razão de negligência, imprudência, imperícia, incapacidade, dolo ou má-fé, ou ainda, por descumprimento de qualquer cláusula ou condição prevista neste instrumento, por parte da CONTRATADA, esta, obriga-se a responder regressivamente pelos prejuízos causados.

10.5 A tolerância quanto a eventuais infrações do presente contrato não constituirá novação ou renúncia dos direitos conferidos a ambas as partes e/ou aos seus sucessores.

10.6 A CONTRATADA declara que não realizará nenhum investimento para prestação de serviço, objeto deste contrato.

CLÁUSULA DÉCIMA PRIMEIRA – DO FORO DE ELEIÇÃO

11.1 Fica eleito o Foro da Comarca de Vitória, Estado do Espírito Santo, para dirimir as questões oriundas do presente contrato, renunciando-se, desde já, a qualquer outro Foro.

As Partes, de comum acordo, concordam que o presente termo será assinado eletronicamente por seus representantes legais juntamente com duas testemunhas, nos termos dos artigos 219 e 220 do Código Civil, e do art. 10, parágrafos 1º e 2º da Medida Provisória nº 2.200-2, de 24 de agosto de 2001. Neste sentido, as Partes reconhecem a veracidade, autenticidade, integridade, validade e eficácia deste Instrumento e seus termos, para todos os fins de direito.

Serra/ES, (data).

ASSOCIAÇÃO EVANGÉLICA BENEFICENTE ESPÍRITO SANTENSE

Rodrigo André Seidel

Presidente

RAZÃO SOCIAL

Nome do responsável legal

Cargo