RNP
ORGANIZAÇÃO SOCIAL DO MCTI

Educação, Pesquisa
e Inovação em Rede

Termo Técnico

Pré-requisitos para Implantação de SD-WAN

ADC/13905/2024

Nota de Confidencialidade

Este documento, elaborado pela Rede Nacional de Ensino e Pesquisa (RNP), visa solicitar propostas dos fornecedores para atendimento das necessidades descritas para obtenção de para Implantação de SD-WAN.

Sumário

1. Objetivo

Este documento tem como objetivo fornecer aos fornecedores uma visão clara e detalhada dos pré-requisitos técnicos necessários para a implementação, comissionamento e suporte de soluções SD-WAN em uma rede de hospital público. O intuito é garantir que os fornecedores possam dimensionar adequadamente os equipamentos e soluções necessárias, assegurando uma implantação eficiente e eficaz.

Inicialmente, será realizado um piloto da solução, contemplando 4 unidades, conforme descrito neste termo técnico. Com base no sucesso do piloto, a implantação poderá ser expandida para até 80 unidades. Essa condição deverá ser considerada no dimensionamento dos equipamentos do piloto.

2. Informações Gerais

A RNP, criada em 1989, pelo então Ministério da Ciência e Tecnologia (MCT), desenvolve, mantém e opera uma infraestrutura de Internet acadêmica, conhecida como Rede Ipê, seu *backbone* nacional, consistindo em uma rede de Internet com pontos de presença (PoPs) em todos os 26 estados brasileiros e, adicionalmente, no Distrito Federal, além de conexões diretas à Internet global e às principais redes de ensino e pesquisa da América Latina, América do Norte e Europa, e, a partir destas regiões, ao restante do mundo.

Como associação civil sem fins lucrativos, foi qualificada segundo a Lei 9.637/1998 pela presidência da República, como uma Organização Social vinculada ao Ministério da Ciência, Tecnologia e Inovação (MCTI) e mantida por esse, em conjunto com os ministérios da Educação (MEC), das Comunicações (MCom), Cultura (MinC), Saúde (MS) e Defesa (MD). A RNP é responsável pela execução do Programa Interministerial para o Desenvolvimento e Manutenção da Rede Nacional de Ensino e Pesquisa (PRORNP) de redes para educação e pesquisa.

O PRORNP vem desde 1999 apoiando ações de interiorização da plataforma digital para educação e pesquisa em todo território nacional. Existem cerca de 1.800 campi de organizações usuárias interligadas ao Sistema RNP[1] , compostas por universidades e

[1] Portaria Interministerial no. 3.825, de 12 de dezembro de 2018, atualiza o Programa Interministerial RNP (PRORNP), apontando a Organização Social RNP responsável por desenvolver e manter o Sistema RNP.

instituições de pesquisa, agências de fomento e órgãos de apoio, ambientes de inovação e empresas inovadoras, que utilizam aplicações de comunicação e colaboração para cerca de 4 milhões de alunos, professores e pesquisadores. O Sistema RNP é conformado por um conjunto de redes de comunicação, de campi e metropolitanas, integradas pela Rede Ipê – o Sistema Autônomo Internet, AS 1916.

A Figura 1 a seguir apresenta a Rede Ipê, o *backbone* nacional da RNP.

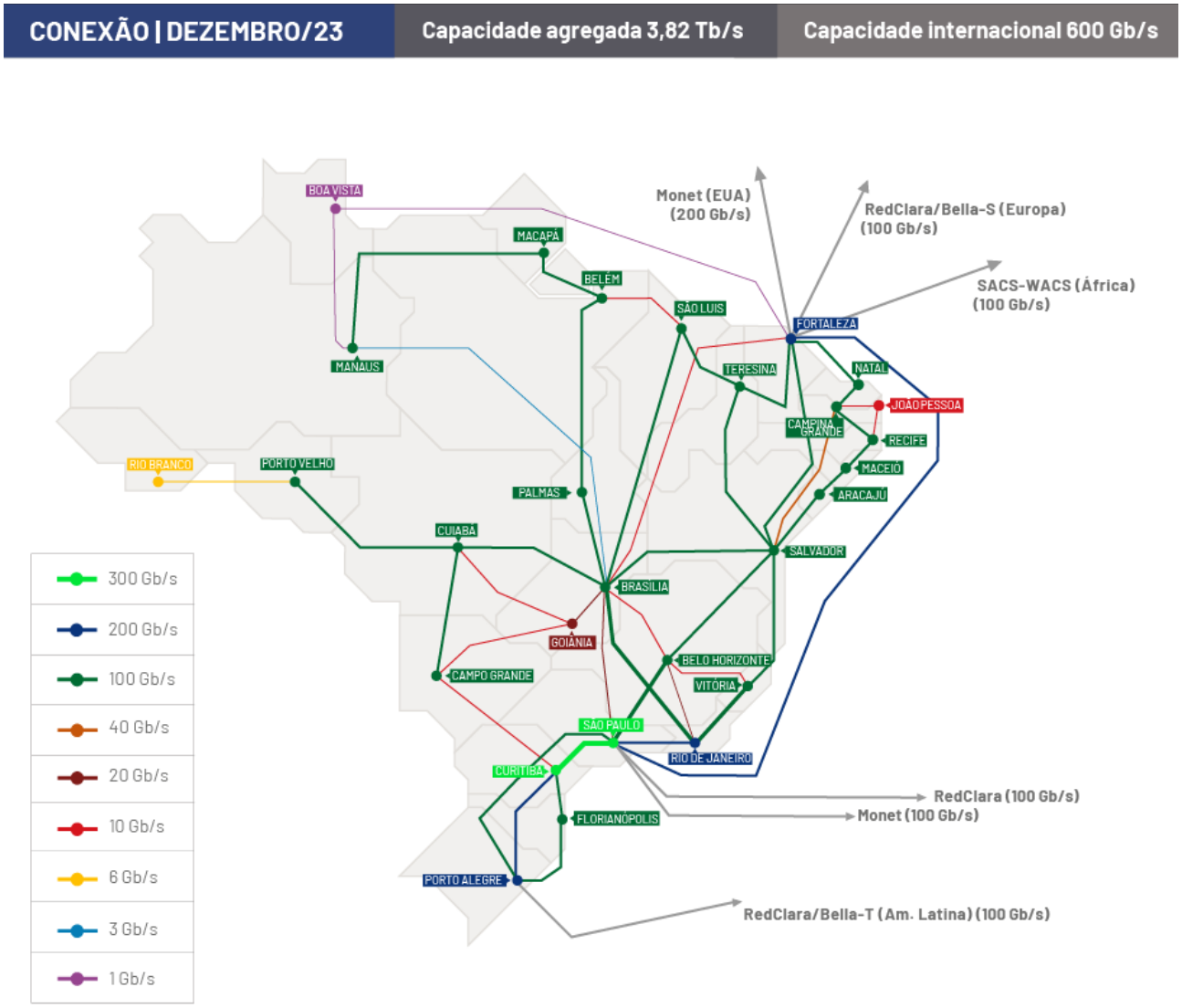

Figura 1: Rede Ipê, o *backbone* nacional da RNP

3. Escopo

Este documento tem como objetivo fornecer aos fornecedores uma visão clara e detalhada dos pré-requisitos técnicos necessários para a implementação, comissionamento e suporte de soluções SD-WAN em quatro unidades de uma rede de

hospital público. O intuito é garantir que os fornecedores possam dimensionar adequadamente os equipamentos e soluções necessárias, assegurando uma implantação eficiente e eficaz.

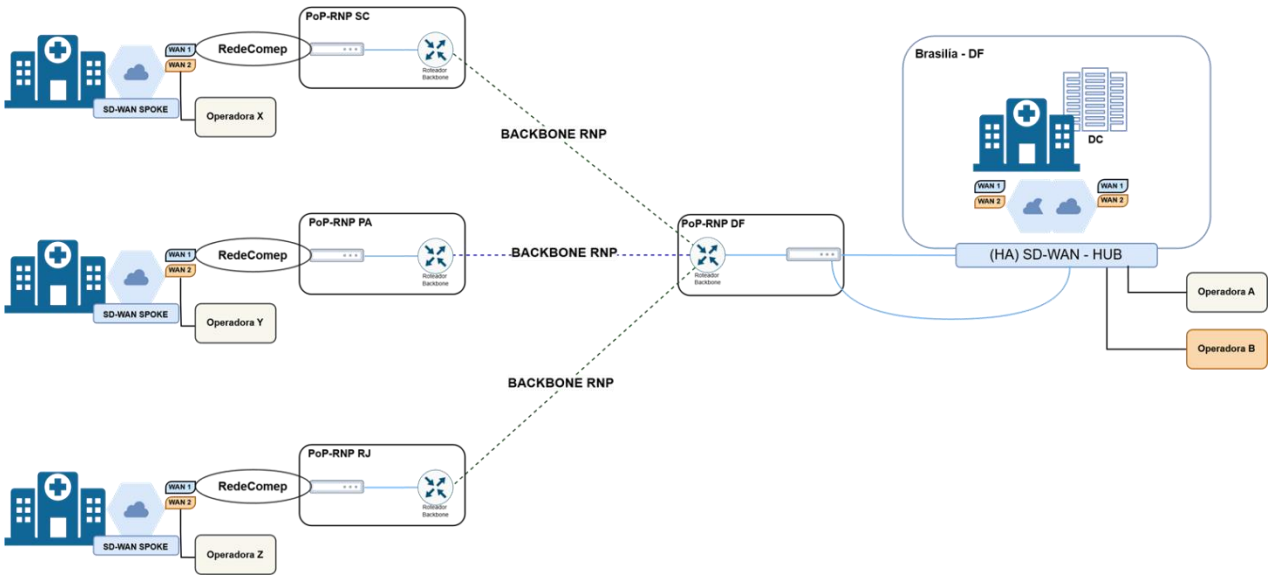

Figura 2 Topologia de referência

Descrição das Unidades e Conectividade Lógica

As unidades hospitalares estão localizadas nas seguintes cidades:

- Brasília
- Florianópolis
- Belém
- Rio de Janeiro

Conectividade Física: Todas as unidades são atendidas por links da *RedeComep*, que são redes comunitárias de educação e pesquisa de alta velocidade, conectadas por Pontos de Presença (PoPs) da RNP nas regiões metropolitanas do país. Além disso, serão contratados links de operadoras de internet banda larga como opção de contingência e resiliência, garantindo a continuidade dos serviços em caso de falhas.

4. Conectividade Redundante e de Alta Disponibilidade:

- Garantir conectividade redundante e de alta disponibilidade entre todas as unidades, utilizando múltiplos links de internet para assegurar a continuidade dos serviços em caso de falhas.

- **Alta Disponibilidade na Unidade de Brasília**: A unidade de Brasília, que possui um datacenter, deve ter alta disponibilidade (HA) para garantir a continuidade dos serviços críticos. Isso inclui redundância de conexões de internet e energia, bem como medidas adicionais de resiliência.

Conectividade Lógica: A conectividade lógica entre as unidades será configurada em uma topologia *full mesh*. Nesta configuração, a unidade de Brasília, que possui um datacenter, atuará como o hub central, enquanto as unidades de Florianópolis, Belém e Rio de Janeiro funcionarão como spokes. Essa estrutura de rede f*ull mesh* assegura alta disponibilidade e redundância, permitindo que cada unidade se comunique diretamente com as outras, minimizando pontos únicos de falha e melhorando a resiliência da rede.

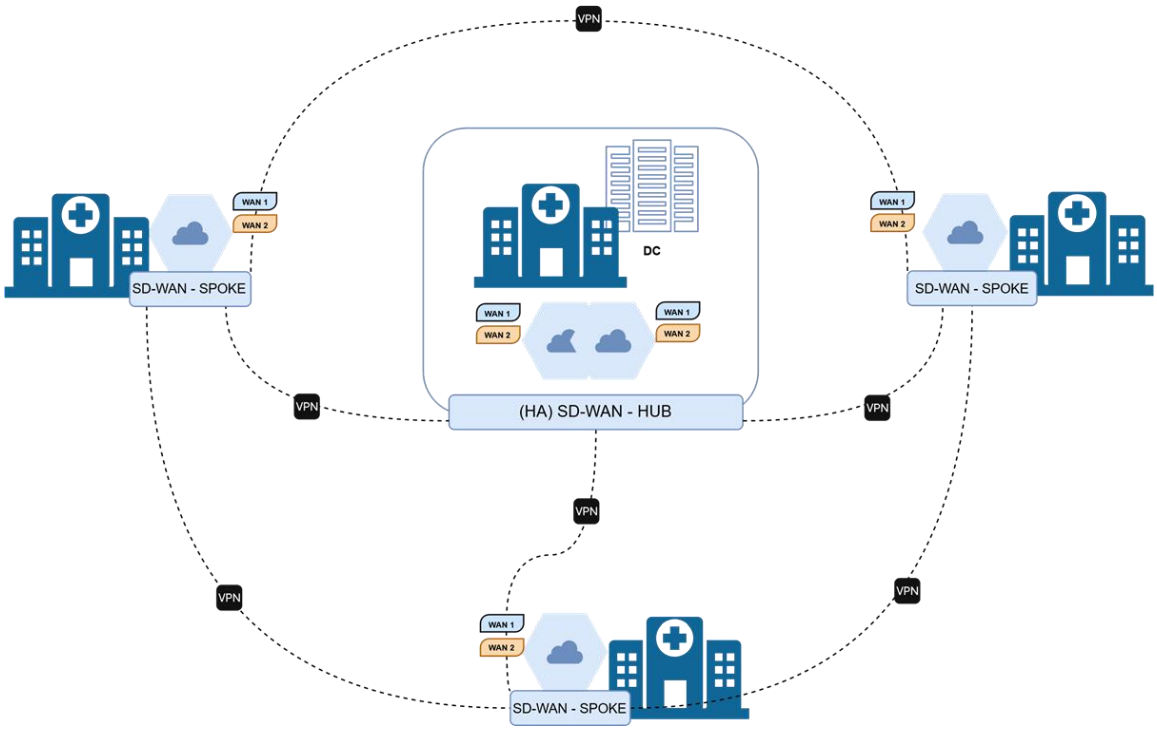

Figura 3 Conectividade entre unidades

Requisitos de Velocidade de Conexão: Inicialmente, as unidades serão atendidas com as seguintes velocidades de conexão:

- Brasília: 4 Gbps
- Considerar solução de alta disponibilidade (HA) nos modos ativo-ativo e ativo-standby.
- Belém: 1 Gbps
- Rio de Janeiro: 1 Gbps
- Florianópolis: 1Gbps

Esses requisitos garantem que cada unidade tenha a capacidade de conexão necessária para suportar suas operações, com opções de alta disponibilidade para a unidade de Brasília, assegurando a resiliência da rede.

VPNs:

- Comunicação Segura e Criptografada: Garantir que todas as comunicações entre as unidades sejam seguras e criptografadas, protegendo os dados contra interceptações e acessos não autorizados.
- Suporte a VPN com NAT Traversal ou protocolo equivalente: As unidades spoke devem ser capazes de estabelecer conexões VPN utilizando o protocolo NAT Traversal (NAT-T) ou protocolo equivalente, mesmo quando estão por trás de um NAT (Network Address Translation), garantindo flexibilidade e compatibilidade em diferentes ambientes de rede.
- Tecnologias de Criptografia Avançada: Utilização de protocolos de criptografia robustos, como IPSec, para assegurar a integridade e a confidencialidade dos dados transmitidos.
- Gerenciamento Centralizado de VPNs: Facilitar a configuração, monitoramento e gerenciamento das conexões VPN através de uma interface centralizada, permitindo uma administração eficiente e segura da rede.

Escalabilidade: A rede deve ser projetada com alta escalabilidade, com potencial para abranger até 80 unidades adicionais, distribuídas em 5 HUBs e 75 Spokes. Os HUBs atuarão como pontos de agregação de tráfego, enquanto os Spokes serão os pontos finais de conexão.

5. Requisitos Técnicos

5.1 Implantação:

Planejamento e Design: Fornecimento de um plano detalhado de implementação, incluindo topologia de rede, configuração de dispositivos e integração com a infraestrutura existente.

Requisitos de Hardware

Os equipamentos necessários para a implementação das soluções SD-WAN devem atender aos seguintes requisitos mínimos:

Interfaces de Rede:

- Mínimo de oito interfaces Ethernet para garantir conectividade adequada e flexível com outros dispositivos de rede.
- Mínimo de duas interfaces WAN para assegurar redundância e alta disponibilidade das conexões de internet.
- Suporte para interfaces Gigabit Ethernet (1 Gbps) e, preferencialmente, interfaces 10 Gigabit Ethernet para conexões de alta velocidade

5.2 Desempenho:

Throughput mínimo de 1 Gbps para suportar o tráfego de dados necessário sem comprometer a performance da rede.

Power over Ethernet (PoE):

Interface PoE para fornecer energia a dispositivos compatíveis diretamente através do cabo Ethernet, simplificando a instalação e reduzindo a necessidade de fontes de alimentação adicionais.

Segurança:

- Suporte a firewall integrado para proteção avançada contra ameaças, incluindo inspeção de pacotes, prevenção de intrusões e controle de acesso.
- Suporte a IPSec ou protocolos equivalentes que garantam a segurança das comunicações através de criptografia robusta. Isso assegura a integridade e a confidencialidade dos dados transmitidos, protegendo contra interceptações e acessos não autorizados em diversos ambientes de rede.

Wireless (desejável):

- Suporte a Wi-Fi 6 (802.11ax) para garantir alta velocidade e eficiência na conectividade sem fio.
- Múltiplas antenas MIMO (*Multiple Input Multiple Output*) para melhorar a cobertura e a capacidade da rede wireless.
- Capacidade de gerenciar múltiplos SSIDs (*Service Set Identifiers*) para segmentar diferentes tipos de tráfego e usuários.

Switch:

- Suporte a switching Layer 2 e Layer 3 para permitir roteamento e comutação eficientes dentro da rede.
- Capacidade de VLAN (Virtual Local Area Network) para segmentação de rede e melhor gerenciamento de tráfego.
- Suporte a QoS (Quality of Service) para priorização de tráfego crítico e garantia de desempenho consistente.

VPN:

Capacidade de suportar o número de VPNs simultâneas, considerando a projeção da rede detalhada neste documento, para permitir conexões seguras entre múltiplos pontos da rede.

Conectividade LTE:

Dispositivo específico para conexão LTE que suporte tecnologias 4G e 5G, proporcionando uma alternativa de conectividade móvel de alta velocidade.

6. Requisitos de Software

Os softwares necessários para a operação dos equipamentos SD-WAN devem atender aos seguintes requisitos mínimos:

- **Licenciamento**:
  - Todas as licenças de software necessárias para a operação dos equipamentos SD-WAN devem ser fornecidas sem limitação de licença e sem custos adicionais. Isso inclui quaisquer atualizações ou upgrades necessários durante o período de suporte.
- **Configuração Inicial**:
  - A configuração inicial dos dispositivos SD-WAN deve incluir:
  - Políticas de roteamento para garantir a eficiência e a segurança do tráfego de rede.
  - Configurações de QoS (Qualidade de Serviço) para priorizar o tráfego crítico e garantir a qualidade das aplicações essenciais.
  - Balanceamento de carga para distribuir o tráfego de rede de forma equilibrada entre os links disponíveis, otimizando o desempenho e a redundância.
- **Interface de Configuração**:

- As configurações dos dispositivos SD-WAN devem ser realizadas através de um dashboard intuitivo ou via API, permitindo uma gestão simplificada e eficiente.

- **Gerenciamento em Nuvem**:
  - O gerenciamento dos dispositivos SD-WAN deve ser 100% em nuvem, proporcionando acesso remoto, monitoramento em tempo real e atualizações automáticas. Isso garante maior flexibilidade e facilidade na administração da rede.

7. Segurança

Para garantir a proteção e integridade da rede SD-WAN, os fornecedores devem atender aos seguintes requisitos de segurança:

- **Firewall**:
  - Integração de capacidades de firewall avançadas, incluindo:
  - Inspeção de pacotes para monitorar e filtrar o tráfego de rede em tempo real.
  - Prevenção de intrusões (IPS) para detectar e bloquear tentativas de ataque.
  - Controle de acesso para definir políticas de segurança que restrinjam o acesso a recursos críticos da rede.
- **IPS (Intrusion Prevention System.)**
  - Implementação de um IPS para detectar atividades suspeitas e tomar medidas imediatas para bloquear essas ameaças em tempo real. O IPS deve ser capaz de:
  - **Mitigação Automática:** Aplicação de políticas de segurança automaticamente para mitigar ataques, incluindo a atualização de regras de firewall, a aplicação de patches de segurança e a execução de scripts de resposta a incidentes.
- **Análise Comportamental**: Utilização de técnicas de análise comportamental para identificar e bloquear ameaças desconhecidas ou de dia zero.
- **IDS (Intrusion Detection System):**
  - Implementação de um sistema de detecção de intrusões (IDS) para monitorar e analisar o tráfego de rede em busca de atividades suspeitas ou maliciosas. O IDS deve ser capaz de:

- Detectar tentativas de intrusão e ataques em tempo real.
- Gerar alertas automáticos para incidentes de segurança.
- Fornecer relatórios detalhados sobre eventos de segurança detectados.

- **SASE (Secure Access Service Edge):**
  - Integração de SASE para combinar funções de rede e segurança em uma única plataforma, proporcionando acesso seguro e eficiente a recursos distribuídos.
- **ZTNA (Zero Trust Network Access):**
  - Implementação de ZTNA para garantir que o acesso à rede seja concedido com base em políticas de confiança zero, verificando continuamente a identidade e o contexto dos usuários e dispositivos.
- **CABS (Cloud Access Security Broker):**
  - Utilização de CABS para monitorar e controlar o uso de serviços em nuvem, garantindo a conformidade com políticas de segurança e protegendo dados sensíveis.
- **VPN**:
  - Suporte a VPNs seguras para comunicação entre os pontos da rede, garantindo a criptografia de ponta a ponta dos dados transmitidos. Isso inclui:
    - Suporte a IPSec para estabelecer conexões VPN seguras.
    - Capacidade de suportar a quantidade de VPNs simultâneas, descrita nas especificações desse documento, para permitir conexões seguras entre múltiplos pontos da rede.
- **Compliance**:
  - Conformidade com normas e regulamentos de segurança, como:
    - LGPD (Lei Geral de Proteção de Dados Pessoais) para garantir a proteção dos dados pessoais.
    - ISO 27001 para assegurar a implementação de um sistema de gestão de segurança da informação.
    - Outras normas relevantes que garantam a segurança e a privacidade dos dados.
- **Relatórios de Segurança**:
  - Geração de relatórios detalhados sobre a segurança da rede, incluindo:

- Relatórios de uso e consumo para monitorar a utilização dos recursos da rede.
- Relatórios de incidentes de segurança para documentar e analisar tentativas de ataque e violações de segurança.
- Relatórios de conformidade para demonstrar a adesão às normas e regulamentos de segurança.
- Relatórios de acesso à Internet por usuários: Implementação de um sistema de relatórios detalhados sobre o acesso à internet por usuários, permitindo a análise e auditoria de atividades online para identificar e mitigar riscos de segurança.

- **Atualizações de Segurança**:
  - Implementação de um processo contínuo de atualizações de segurança para garantir que todos os dispositivos SD-WAN estejam protegidos contra as últimas ameaças e vulnerabilidades. Isso inclui:
    - Atualizações regulares de firmware e software.
    - Aplicação de patches de segurança assim que disponíveis.
- **Monitoramento de Segurança**:
  - Monitoramento contínuo da rede para detectar e responder a ameaças em tempo real. Isso inclui:
    - Sistemas de detecção e resposta a incidentes (IDR) para identificar e mitigar ameaças rapidamente.
    - Análise de tráfego de rede para identificar padrões suspeitos e atividades maliciosas.

8. Adequação dos Sites

8.1 Requisitos para Adequação dos Sites

Para garantir a estabilidade e continuidade da operação das soluções SD-WAN, é necessário realizar uma avaliação (*site survey*) e adequação dos sites onde os equipamentos serão instalados. Os requisitos mínimos para essa adequação incluem:

- **Avaliação do Site**:
  - Realizar uma avaliação detalhada do site para identificar as necessidades específicas de infraestrutura e garantir que o ambiente esteja preparado para a instalação dos equipamentos SD-WAN.

- **Instalação de No-breaks**:
    - Instalar no-breaks (UPS) para fornecer energia ininterrupta aos equipamentos, garantindo que eles continuem operando durante quedas de energia ou flutuações na rede elétrica.
- **Réguas de Energia**:
    - Instalar réguas de energia adequadas para distribuir a energia de forma segura e eficiente aos equipamentos. As réguas devem ter proteção contra surtos e capacidade suficiente para suportar todos os dispositivos conectados.

9. Comissionamento

O processo de comissionamento das soluções SD-WAN deve incluir as seguintes etapas:

- **Testes de Aceitação**:
    - Realização de testes de aceitação para validar a funcionalidade e o desempenho da solução SD-WAN. Esses testes devem garantir que todos os componentes do sistema estejam operando conforme especificado e que a rede atenda aos requisitos de desempenho e segurança estabelecidos.
- **Documentação**:
    - Fornecimento de documentação completa e detalhada da configuração e dos procedimentos de comissionamento. A documentação deve incluir:
        - Diagramas de topologia de rede.
        - Configurações de dispositivos.
        - Políticas de segurança e roteamento.
        - Procedimentos de backup e recuperação.
        - Instruções detalhadas para a operação e manutenção dos equipamentos.
- **Treinamento**:
    - Treinamento da equipe de TI do cliente para a operação e manutenção da solução SD-WAN. O treinamento deve abranger:
        - Configuração e gerenciamento dos dispositivos SD-WAN.
        - Monitoramento e resolução de problemas.
        - Atualizações de software e manutenção preventiva.

    - Melhores práticas de segurança e gestão de rede.
- **Entrega e Instalação**:
    - Coordenação da entrega e instalação dos equipamentos nos locais designados. Isso inclui a verificação de que todos os componentes foram entregues conforme especificado e a instalação física dos dispositivos.
- **Configuração Inicial**:
    - Configuração inicial dos dispositivos SD-WAN, incluindo a aplicação de políticas de roteamento, QoS (Qualidade de Serviço) e balanceamento de carga. As configurações devem ser realizadas de acordo com as especificações do projeto e as necessidades do cliente.
- **Verificação de Conectividade**:
    - Verificação da conectividade entre todas as unidades, garantindo que a topologia full mesh esteja operando corretamente e que a unidade de Brasília esteja funcionando como o hub central.

10. Suporte

Para garantir a operação contínua e eficiente das soluções SD-WAN, os fornecedores devem oferecer os seguintes serviços de suporte:

- **Períodos de Suporte**:
    - Oferecimento de contratos de suporte para períodos de 1, 3 e 5 anos, com opções de suporte 24/7.
- **Monitoramento e Gestão**:
    - Serviços de monitoramento proativo e gestão da rede SD-WAN, incluindo:
        - Detecção e resolução de problemas em tempo real.
        - Monitoramento contínuo do desempenho da rede e dos dispositivos.
        - Alertas automáticos para eventos críticos e anomalias.
        - Relatórios regulares sobre o estado da rede e o desempenho dos dispositivos.
- **Atualizações e Manutenção**:
    - Atualizações regulares de software para garantir que os dispositivos SD-WAN estejam sempre protegidos contra vulnerabilidades e operando com as últimas melhorias de desempenho e funcionalidades.

- Manutenção preventiva dos equipamentos para evitar falhas e prolongar a vida útil dos dispositivos. Isso inclui inspeções regulares, limpeza, e substituição de componentes desgastados.

- **Suporte Técnico**:
  - Acesso a suporte técnico especializado para resolver problemas complexos que não possam ser solucionados pelo monitoramento e gestão proativa. Isso inclui:
    - Atendimento via telefone, e-mail e chat.
    - Suporte remoto para diagnóstico e resolução de problemas.
    - Visitas técnicas ao local, se necessário, para resolver problemas críticos.
- **Treinamento e Capacitação**:
  - Treinamento contínuo da equipe de TI do cliente para garantir que eles estejam atualizados com as melhores práticas de operação e manutenção da solução SD-WAN. Isso pode incluir:
    - Sessões de treinamento presenciais e online.
    - Acesso a materiais de treinamento e documentação atualizada.
    - Workshops e webinars sobre novos recursos e atualizações de software.
- **Relatórios e Análises**:
  - Geração de relatórios detalhados sobre o uso da rede, desempenho dos dispositivos, e incidentes de segurança. Esses relatórios devem ser fornecidos regularmente e incluir análises que ajudem o cliente a otimizar a operação da rede e planejar futuras expansões.

11. Considerações Finais

Os fornecedores interessados devem apresentar uma proposta detalhada que aborde todos os pré-requisitos mencionados neste documento. A proposta deve incluir:

- **Cronograma de Implementação**:
  - Um plano detalhado com as etapas de implementação, desde a entrega dos equipamentos até a conclusão do comissionamento e início da operação.
- **Custos**:
  - Uma estimativa detalhada dos custos envolvidos, incluindo:

- Custos de aquisição dos equipamentos.
- Custos de licenciamento de software.
- Custos de instalação e configuração.
- Custos de suporte e manutenção para os períodos de 1, 3 e 5 anos.

- **Referências de Projetos Similares**:
  - Exemplos de projetos anteriores semelhantes, incluindo detalhes sobre a escala do projeto, os desafios enfrentados e os resultados alcançados. Isso ajudará a demonstrar a experiência e a capacidade do fornecedor em entregar soluções SD-WAN de alta qualidade.
- **Garantias e SLAs**:
  - Detalhes sobre as garantias oferecidas para os equipamentos e serviços, bem como os Acordos de Nível de Serviço (SLAs) que garantem a qualidade e a disponibilidade dos serviços prestados.
- **Equipe Técnica**:
  - Informações sobre a equipe técnica que será responsável pela implementação e suporte da solução, incluindo qualificações, certificações e experiência relevante.

12. Fluxo do Processo

Este processo será dividido da seguinte maneira:

Etapa	Descrição
Workshop	RNP convida integradores para apresentação do projeto.
Convite	RNP convida integradores.
Aceite	Integradores aceitam o convite, tornando-se proponentes
Esclarecimentos	RNP esclarece dúvidas dos proponentes
Propostas	Integradores proponentes enviam propostas para RNP
Análise	RNP analisa propostas e seleciona provedores qualificados
Negociação técnica/comercial	RNP e integradores selecionados detalham propostas e negociam condições do projeto.
Assinatura	RNP e integrador selecionado assinam acordo.

13. Condições de pagamento

Como regra geral, o término de cada mês a empresa deverá enviar ao gestor responsável pela iniciativa a solicitação de faturamento, descrevendo o volume de entregas executadas ou horas realizadas por cada um dos profissionais contratados para atuação na demanda. Sendo cumprido o volume de horas ou escopo acordado e atendido os padrões de qualidade definidos, o gestor da iniciativa terá condições de realizar a aprovação da entrega e, apenas após manifestação da aprovação, a empresa poderá realizar o envio da nota fiscal.

Os pagamentos serão efetuados pela RNP nos dias 05 e 20 do mês e condicionados as seguintes regras:

a) Prazo mínimo para pagamento de 45 dias da emissão da fatura/nota fiscal, desde que os produtos tenham entrega física no local acordado em pedido com até 20 (vinte) dias uteis de antecedência do vencimento da fatura.

b) As Notas Fiscais (eletrônicas) ou Faturas devem ser entregues com pelo menos 20 (vinte) dias uteis de antecedência de seu vencimento. Caso não seja entregue nesse período, o pagamento será transferido para a data mais próxima de acordo com a regra de pagamento da RNP.

c) Os pagamentos relativos a serviços somente serão liberados após o aceite formal da área demandante da RNP (Gestor responsável).

14. Documentação necessária para homologação administrativa

1. CNPJ com atividade econômica de acordo com os serviços a serem prestados para RNP;
2. Prova de regularidade relativa à Seguridade Social, comprovada pela Certidão Negativa de Débito (C.N.D), expedida pelo INSS;
3. Prova de regularidade com o Fundo de Garantia por Tempo de Serviço (FGTS), comprovada pela Certidão de Regularidade de Situação (C.R.S.);
4. Certidão Negativa de Débitos Trabalhistas;
5. Cópia do Contrato Social e alterações contratuais.