Estudo Técnico Preliminar 22/2024

1. Informações Básicas

Número do processo: 25100.000202/2024-30

2. Descrição da necessidade

A Fundação Nacional de Saúde (Funasa), órgão executivo do Ministério da Saúde, tem como missão, promover a saúde pública e a inclusão social por meio de ações de saneamento e saúde ambiental, por isso vem trabalhando no aprimoramento das políticas, diretrizes e instrumentos de apoio à gestão. Nesse contexto, a tecnologia da informação é estratégica e imprescindível para a consolidação de um sistema de informação, para resolubilidade das ações e serviços de saneamento e saúde ambiental em todo o território nacional.

Atualmente a Funasa conta com o contrato nº 50/2018, para prestação de serviços de rede IP de Multisserviços contemplando o fornecimento de link de internet, link de rede MPLS e pontos de acesso de forma a prover transmissão de dados, voz e vídeo entre as unidades da FUNASA - Processo SEI nº 25100.006435/2016-36. O contrato fora prorrogado de forma excepcional por 12 (doze) meses, até 10/07/2024, não cabendo mais prorrogação de vigência, sendo necessária a realização de uma nova contratação.

O objeto é a contratação de fornecimento de link de internet, link de rede MPLS para as unidades da Funasa, incluindo instalação, configuração, repasse de conhecimento, garantia e suporte técnico conforme condições, quantidades, exigências e estimativas estabelecidas neste instrumento.

Motivação / Justificativa

A Rede Corporativa da FUNASA provê infraestrutura física e lógica para que todos os serviços, como acesso à Internet, Intranet, Aplicações Web, correio eletrônico, transferência de arquivos, autenticação de usuários, integração de sistemas, gerência e segurança da informação, VoIP (voz sobre IP), vídeo conferência, dentre outros, possam ser utilizados e, ainda, normatizados e padronizados em todos os pontos remotos da FUNASA. As informações são processadas em tempo real e apresentam um volume de tráfego elevado em determinados pontos cuja disponibilidade é crítica.

A FUNASA atualmente dispõe de 48 links MPLS e 1 link de internet que atende todas as unidades da federação, incluindo as Superintendências Estaduais e as unidades descentralizadas. O contrato atual já apresenta um quantitativo elevado de utilização de serviços, o que tem ocasionado necessidade de ampliação de sua capacidade, como demonstrado ao longo desse documento.

Link de internet

O link de internet atual possui velocidade de 600 Mbps, contudo essa disponibilidade de velocidade já se mostra insuficiente, pois houve um aumento significativo da demanda de Internet da Fundação, desde a contratação realizada em 2018. Esta situação justifica-se pelo aumento do consumo dos serviços em nuvem (Office 365) mas, principalmente, o incremento exponencial de chamadas de videoconferência (potencializados pela pandemia de COVID-19), e com a adoção do teletrabalho parcial ou integral.

Desta forma, há evidente necessidade de contratação de serviço de acesso à Internet, com taxa de transmissão e mecanismos de defesa e prevenção de ataques e com capacidade de absorção do tráfego de Internet consumido em suas atividades diárias, como forma de garantir a continuidade, o atendimento às atividades atuais e previstas da Funasa e o cumprimento de sua missão institucional, dada a atual dependência de seus processos aos serviços de TI associados, observados os princípios de segurança da informação e comunicações na prestação de ambos os serviços.

3. Área requisitante

Área Requisitante	Responsável
DEADM / CGMTI	Raquel Marra Molina de Aguiar - Coordenadora Geral de Modernização e Tecnologia da Informação - Substituta

4. Descrição dos Requisitos da Contratação

4.1. Necessidades Tecnológicas

A partir da análise das necessidades de negócio identificou-se as necessidades tecnológicas a serem atendidas pela presente contratação, nas quais serão necessários o uso de diversas tecnologias de conectividade para o fornecimento de internet, tendo em vista a capilaridade e descentralização dos ambientes, indica-se:

- Serviço de comunicação de dados que permita o tráfego de dados destinados à rede mundial de computadores (Internet), com o uso de tecnologia Fibra Óptica;
- Serviço de comunicação de dados que permita o troca de tráfego corporativo, com o uso de tecnologia Tecnologia Lan To Lan;
- Serviço de comunicação de dados que permita o tráfego de dados, voz e vídeo de abrangência nacional, por meio de uma rede IP multisserviços, em Multi Protocol Label Switching (MPLS);

É necessário que a solução possua segurança para os dados e informações que transitam entre os ambientes da Fundação, em âmbito nacional. Nesse sentido os links de dados devem contemplar tecnologias que implementem requisitos de segurança do tipo:

- Utilização de tecnologias que permitam a construção de uma REDE REMOTA (WAN), de forma a viabilizar:
  - A independência e flexibilidade na transmissão de dados;
  - O uso de protocolos de transmissão que fornecem redundância e desempenhos contínuos;
  - A criação de redes de longa distância com tráfego de dados em uma rede WAN;
  - A conexão de qualquer dispositivo ou aplicativo, independente da sua localização;
- Um serviço de transporte de dados mais viável no momento da conexão, que pode ser uma ligação à internet de banda larga, celular, ou até MPLS (Multiprotocol Label Switching), por exemplo, ocorrerá a conexão com o outro sistema. Isso sempre de acordo com as mais atuais políticas de atuação e de maneira mais econômica possível dentro do tráfego de dados; e
- A simplificação da rede de dados e utilizar recursos de criptografia e firewall, centralizando e homogeneizando o gerenciamento de segurança, possibilitando, ainda, a formatação do tráfego, incluindo regras em torno do tipo de tráfego, tornando-o mais seguro;

É necessário que a solução possua os seguintes requisitos:

- Seja fornecida com todos os equipamentos para a recepção e transmissão dos dados e informações;
- Serviço de monitoramento da disponibilidade de tráfego de dados, segurança dos acessos, monitoramento de incidentes de segurança, ações de contenção e mitigação destes incidentes;
- Controle sobre as tarefas de configuração e gerenciamento em comparação com as redes tradicionais, inclusive com rastreabilidade do consumo de internet;
- Central de atendimento de demandas, reclamações e acompanhamento dos chamados relativos à prestação do serviço de comunicação da rede da Funasa.
- Estrutura que permita o controle da segurança física e lógica de seus ambientes operacionais, estabelecendo as políticas de segurança a serem aplicadas aos serviços de telecomunicações contratados visando a prevenção de incidentes de segurança.

4.2. Demais Requisitos Necessários e Suficientes à Escolha da Solução de TIC

A Solução deverá abranger o fornecimento de software e hardware necessários para o perfeito funcionamento da rede corporativa de dados da Funasa.

Os serviços devem englobar a instalação, configuração de equipamentos e de enlaces de comunicação.

Os planos de implantação e migração deverão prever a conectividade temporária entre as atuais redes corporativas da Funasa e a solução proposta pela CONTRATADA, garantindo a migração sem a interrupção dos serviços existentes.

A execução dos serviços pela contratada deve ser precedido de um Projeto Executivo de rede, a ser analisado pela equipe técnica da Funasa para aprovação. Esse documento deverá conter no mínimo:

- Definição de topologia física e lógica;
- Plano de Implantação e Migração da Rede;
- Cronograma de Implantação da Rede;
- Plano de Endereçamento;
- Plano de balanceamento do tráfego;
- Parâmetros de qualidade de serviço; e
- Dimensionamento de enlaces e interfaces de comunicação.

Deverá ser previsto o repasse de conhecimento sobre a solução implantada na Funasa, com enfoque no funcionamento, configuração e monitoramento dos equipamentos.

4.2.1. Informações Relevantes para o Dimensionamento e/ou Apresentação da Proposta:

A proposta deve ser elaborada utilizando o Anexo I - Modelo de Planilha de Custos e Formação de Preços.

Para o correto dimensionamento e elaboração de sua proposta, o licitante poderá realizar vistoria técnica nas instalações do local de execução dos serviços.

Durante o prazo de elaboração de propostas, ficarão disponíveis os locais onde serão executados os serviços para realização de vistorias técnicas agendadas, para fins de conhecimento da natureza, da área e das condições de sua execução.

As vistorias técnicas serão agendadas na CGMTI, por meio do e-mail cgmti@funasa.gov.br.

Não tendo realizado a vistoria de que trata este título, a licitante não poderá arguir desconhecimento do local, da área ou da infraestrutura existente.

A não realização da vistoria, quando facultativa, não poderá embasar posteriores alegações de desconhecimento das instalações, dúvidas ou esquecimentos de quaisquer detalhes dos locais da prestação dos serviços, devendo a licitante vencedora assumir os ônus dos serviços decorrentes.

A licitante deverá declarar que tomou conhecimento de todas as informações e das condições locais para o cumprimento das obrigações objeto da licitação.

4.3. Locais de instalação:

O serviço de acesso à Internet deverá ser instalado nos endereços discriminados no Anexo XI - Locais de instalação.

4.4. Necessidades de adequação do ambiente para execução contratual:

a) Infraestrutura tecnológica:

O serviço a ser contratado será prestado pela empresa, portanto não existe a necessidade de adequação da infraestrutura tecnológica, tendo em vista que é de responsabilidade da contratada o fornecimento de todo cabeamento necessário desde o distribuidor geral (DG), onde será entregue o acesso a CONTRATADA, até o local definido para o rack, que irá suportar os equipamentos necessários ao funcionamento dos circuitos (modem, roteadores, etc.), bem como eventuais adaptações nas instalações físicas das Unidades (passagem de cabos, lançamento de fibras ópticas, etc.).

O rack que suportará os equipamentos será disponibilizado pela FUNASA.

Serão utilizados os racks já existentes nas unidades que suportam a atual solução.

b) Infraestrutura elétrica:

Como a FUNASA já possui infraestrutura elétrica que suporta a solução atual, inicialmente, não há necessidade de adequação.

Após a apresentação do Plano de Implantação pela contratada, caso seja necessário adequações, a área administrativa (CGLOG) procederá estudo para as devidas adequações.

c) Logística:

A logística para entrega da solução é de responsabilidade da contratada.

d) Espaço físico:

As unidades da FUNASA possuem espaço físico definido para suportar a atual solução, não se vislumbra inicialmente alteração desses espaços.

Após a apresentação do Plano de Implantação pela contratada, caso seja necessário adequações, a área administrativa (CGLOG) procederá estudo para as devidas adequações.

e) Mobiliário:

Não se aplica.

5. Requisitos Legais

- Lei nº 14.133 de 01 de abril ed 2021 – Estabelece normas gerais de licitação e contratação para as Administrações Públicas diretas, autárquicas e fundacionais da União, dos Estados, do Distrito Federal e dos Municípios;
- Lei nº 10.520, de 17 de julho de 2002 – Institui, no âmbito da União, Estados, Distrito Federal e Municípios, nos termos do art. 37,inciso XXI, da Constituição Federal, modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns, e dá outras providências;
- Lei Complementar nº 123, de 14 de dezembro de 2006 - Institui o Estatuto Nacional da Microempresa e da Empresa de Pequeno Porte; altera dispositivos das Leis nº 8.212 e 8.213, ambas de 24 de julho de 1991, da Consolidação das Leis do Trabalho - CLT, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943, da Lei nº 10.189, de 14 de fevereiro de 2001, da Lei Complementar nº 63, de 11 de janeiro de 1990; e revoga as Leis nº 9.317, de 5 de dezembro de 1996, e 9.841, de 5 de outubro de 1999, e suas alterações;
- Decreto nº 9.507, de 21 de setembro de 2018 - Dispõe sobre a execução indireta, mediante contratação, de serviços da administração pública federal direta, autárquica e fundacional e das empresas públicas e das sociedades de economia mista controladas pela União;
- Decreto nº 10.024, de 20 de setembro de 2019 – Regulamenta o pregão, na forma eletrônica, para aquisição de bens e serviços comuns, e dá outras providências;
- Decreto nº 7.174, de 12 de maio de 2010 – Regulamenta a contratação de bens e serviços de informática e automação pela administração pública federal, direta ou indireta, pelas fundações instituídas ou mantidas pelo Poder Público e pelas demais organizações sob o controle direto ou indireto da União;
- Instrução Normativa nº 05 de 26 de maio de 2017, que dispõe sobre as regras e diretrizes do procedimento de contratação de serviços sob o regime de execução indireta no âmbito da Administração Pública Federal direta, autárquica e fundacional da Secretaria de Gestão do Ministério do Planejamento, Desenvolvimento e Gestão;
- Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2023, que dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal da Secretaria de Governo Digital do Ministério da Economia;
- Instrução Normativa nº 73, de 05 de agosto de 2020 que dispõe sobre o procedimento administrativo para a realização de pesquisa de preços para a aquisição de bens e contratação de serviços em geral;
- Resolucaõ nº 717, de 23 de dezembro de 2019 Anatel - Aprova o Regulamento de Qualidade dos Serviços de Telecomunicacoẽs -RQUAL;

- Decreto nº 9.450/2018 que institui a Política Nacional de Trabalho no âmbito do Sistema Prisional, voltada à ampliação e qualificação da oferta de vagas de trabalho, ao empreendedorismo e à formação profissional das pessoas presas e egressas do sistema prisional, e regulamenta o § 5º do art. 40 da Lei nº 8.666, de 21 de junho de 1993, que regulamenta o disposto no inciso XXI do caput do art. 37 da Constituição e institui normas para licitações e contratos da administração pública firmados pelo Poder Executivo Federal:
    - A contratação proposta trata de serviços de comunicação, contemplando a utilização de infraestrutura da CONTRATADA, possuindo características de serviço continuado, não requerendo, necessariamente, novos postos de trabalho; e
    - O artigo 5º, § 4º, do Decreto em tela, prevê que a "administração pública poderá deixar de aplicar o disposto neste artigo quando, justificadamente, a contratação de pessoa presa ou egressa do sistema prisional se mostrar inviável", nesta hipótese caberá a CONTRATADA demonstrar tal inviabilidade.

6. Requisitos de Segurança

O Contratado deverá observar integralmente os requisitos de Segurança da Informação e Privacidade descritos a seguir:

- Deverão ser observados os regulamentos, normas e instruções de segurança da informação e comunicações adotadas pela FUNASA, incluindo, mas não se limitando, ao definido na Política de Segurança da Informação e Comunicações e suas Normas Complementares, durante a execução dos serviços nas instalações da FUNASA.
- Deverá ser garantida a disponibilidade, integridade, confidencialidade e sigilo dos documentos e informações inerentes ao contrato e seus serviços, podendo ser responsabilizado legalmente quem porventura causar perdas e danos à FUNASA e a terceiros.
- Toda informação confidencial gerada e/ou manipulada em razão desta contratação, seja ela armazenada em meio físico, magnético ou eletrônico, deverá ser devolvida nas seguintes hipóteses, mediante formalização entre as partes.
    - Término ou rompimento do Contrato; ou
    - Solicitação da FUNASA.
- Devem ser utilizadas ferramentas de proteção e segurança de informações, a fim de evitar qualquer acesso não autorizado aos sistemas e softwares, seja em relação ao que eventualmente estejam sob sua responsabilidade direta ou que foram disponibilizados a FUNASA, ainda que por meio de link.
- Quando solicitado formalmente pela FUNASA, deverão ser realizadas, prioritária e concomitantemente, alterações para sanar possíveis problemas de segurança ou de vulnerabilidade nos referidos sistemas ou softwares utilizados para execução do serviço contratado.
- A CONTRATADA deverá informar à FUNASA, formalmente e tempestivamente, sobre quaisquer necessidades de atualização ou mudança na configuração dos serviços prestados.
- Executar os serviços em conformidade com a legislação aplicável, em especial, ABNT NBR ISO/IEC 27002:2013.
- Prestar os esclarecimentos necessários à FUNASA, bem como informações concernentes à natureza e andamento dos serviços executados, ou em execução.
- Garantir a integridade e disponibilidade dos documentos e informações que, em função do Contrato, estiverem sob a sua guarda, sob pena de responder por eventuais perdas e/ou danos causados a FUNASA e a terceiros.
- A empresa contratada não poderá divulgar, mesmo que em caráter estatístico, quaisquer informações originadas na FUNASA, sem prévia autorização.
- O acesso às instalações da Contratada onde serão realizados os serviços deverá ser controlado e permitido somente às pessoas autorizadas.
- A Contratada deverá manter os seus profissionais identificados por crachás, quando em trabalho, devendo substituir imediatamente aquele que seja considerado inconveniente à boa ordem ou que venha a transgredir as normas disciplinares da FUNASA.
- A contratada deverá manter os seus profissionais informados quanto às normas disciplinares da FUNASA, exigindo sua fiel observância, especialmente quanto à utilização e segurança das instalações.
- Deverá ser celebrado Termo de Compromisso de Manutenção de Sigilo entre a contratada e a FUNASA para garantir a segurança das informações da FUNASA, assim como, celebrado o Termo de Ciência a todos envolvidos na prestação dos serviços.
- Não transferir a terceiros os serviços contratados.
- Manter sigilo absoluto sobre todas as informações provenientes dos serviços realizados, documentos elaborados e informações obtidas dentro da FUNASA.

7. Requisitos de Sustentabilidade

De acordo com o art. 16, inciso I, alínea “g” da Instrução Normativa SGD/ME nº 94, de 2022, os Requisitos Sociais, Ambientais e Culturais definem os requisitos que a Solução de TIC deve atender para estar em conformidade com costumes, idiomas e ao meio ambiente, dentre outros, observando-se, inclusive, no que couber, o Guia Nacional de Contratações Sustentáveis, e suas atualizações, elaborado pela Câmara Nacional de Sustentabilidade da Controladoria Geral da União/Advocacia Geral da União.

Preferência pelo uso de documentação em formato eletrônico foi adotada, visando minimizar o uso de papel e, portanto, a produção de resíduos de serviços gráficos.

Devido à natureza da contratação, que envolve a contratação de links de internet, com solução composta de equipamentos, onde não serão utilizados equipamentos ou materiais nocivos ao meio ambiente, não se identificou a pertinência de serem definidos critérios ambientais.

Ressalta-se que não foram identificados outros critérios de sustentabilidade aplicáveis na consulta ao Guia Nacional de Contratações Sustentáveis, e suas atualizações, elaborado pela Câmara Nacional de Sustentabilidade da Controladoria Geral da União/Advocacia Geral da União.

8. Levantamento de Mercado

Em fase preliminar da análise foram consideradas as seguintes soluções tecnológicas:

8.1. Link MPLS (Multi – Protocol Label Switching)

O MPLS (Multiprotocol Label Switching) é uma técnica de transporte de dados usada em redes de alto desempenho, essencialmente, é um protocolo para acelerar e moldar o fluxo de rede. Tem por objetivo, garantir um caminho exclusivo dentro de uma rede, representa até hoje a forma mais eficiente de se garantir confiabilidade de dados em comunicação de longa distância e tem sido tradicionalmente usado na maioria dos ambientes de telecomunicações.

Outras características a serem destacadas são, a capacidade de entregar pacotes e fornecer uma alta qualidade de serviço (QoS), excelente em gerenciar e evitar a perda de pacotes, mantem o fluxo de tráfego mais importante de uma empresa, é uma tecnologia de encaminhamento de pacotes baseadas em rótulos ou labels e opera da mesma maneira para switches e roteadores, entre as camadas 2 e 3 do modelo OSI.

Assim os serviços MPLS são capazes de interligar os pontos estratégicos da Funasa, por meio da criação de redes privativas virtuais com acessos dedicados, isolados da internet, com qualidade de serviço e perfis de tráfego adequados às necessidades do negócio. Ou seja, uma rede comum de internet não utiliza esse conceito, já que todos os pacotes são trafegados sem prioridade.

Os grandes benefícios incluem:

1. Tecnologia de encaminhamento de pacotes e rótulos para tomar decisões;
2. Cria previsibilidade de tráfego, o que é útil quando há muitos clientes em uma rede compartilhada;
3. Evita a perda de pacotes e mantendo o fluxo de tráfego;
4. Capacidade de entregar pacotes e fornecer uma alta qualidade de serviço;
5. Segurança; e
6. Mantém a integridade dos dados e informações.

8.2. Tecnologia SD-WAN (Software-Defined Wide Area Network, Rede Definida por Software)

A tecnologia SD-WAN é uma abordagem definida por software (software-defined) para gerenciar uma WAN (widearea network rede de longa distância). Ela surgiu como uma solução para facilitar o gerenciamento da rede de forma remota ou permitir que o próprio sistema execute o melhor percurso de roteamento de rede de forma automática.

Com a SD-WAN, o tráfego é enviado de forma automática pelo melhor caminho da WAN, para isso, o software utiliza informações sobre a qualidade dos links, o tempo de resposta e evita que o roteamento seja feito apenas por protocolo dinâmico. A SD-WAN apresenta maior visibilidade, escalabilidade, controle e desempenho.

É mais fácil e rápido implementar um serviço SD-WAN e, além disso, a largura de banda pode ser adicionada ou reduzida sempre que se entender necessário.

A SD-WAN é a aplicação dos conceitos de SDN (Software Defined Networking) à WAN, isso significa a implantação de dispositivos de borda SD-WAN que aplicam regras e políticas para enviar tráfego pelo melhor caminho, é uma sobreposição independente de transporte que pode encaminhar qualquer tipo de tráfego - incluindo MPLS. A vantagem do SDWAN é que um arquiteto de tráfego WAN corporativo pode se dedicar em um ponto central e aplicar facilmente políticas em todos os dispositivos WAN.

Os grandes benefícios incluem:

1. Maior disponibilidade global;
2. Mantém a integridade dos dados e informações;
3. A largura de banda pode ser adicionada ou reduzida conforme necessidade;
4. Implementa políticas de rede baseadas em gerenciamento centralizado;
5. Direciona tráfego baseado em políticas por aplicação;
6. Aplica o uso inteligente de links com monitoração dinâmica de desempenho e falha;
7. Permite a visibilidade e controle da rede por meio de Portal WEB; e
8. Disponibiliza informações básicas de qualidade e desempenho dos links internet.

8.3. Internet Banda Larga

O Serviço de Internet banda larga consiste em uma rede com vários usuários utilizando o mesmo caminho até o provedor para o acessar a internet, o que acaba a tornando lenta pelo volume de pessoas conectadas. É provido por meio da utilização dos protocolos de Internet IPv4 ou IPv6.

O meio de acesso é compartilhado entre vários usuários havendo uma degradação do sinal nos horários de maior utilização. Conforme regulamentação da Anatel, a operadora deve garantir mensalmente, na média, pelo menos 80% da largura de banda contratada.

Em decorrência do volume de utilização, a tecnologia possui assimetria nas comunicações, ou seja, discrepância quando comparado as taxas de download e de upload, de forma que as taxas de upload são em média equivalente a 10% das taxas de download.

Na internet banda larga não há garantia de fornecimento de banda, nem níveis de qualidade de serviços associados, podem ocorrer oscilações de velocidade e desempenho, dessa forma é indicado para de uso comum, onde a instabilidade de conexão não resulte em prejuízos, **portanto não está em conformidade com a necessidade da instituição.**

8.4. Internet dedicada

Um Link Dedicado, também conhecido como IP dedicado, consiste numa solução para corporações que necessitam de total garantia de velocidade e disponibilidade de conexão à web. Para que ocorra uma conexão com a web, um computador necessita trocar dados e informações com o provedor, o que ocorre por meio de um caminho exclusivo no Link Dedicado, não havendo compartilhamento do meio físico de última milha. Ele possui garantia na banda de transmissão, assim a velocidade contratada é a velocidade entregue, com pequenas perdas inerentes ao protocolo.

Além da garantia de banda, possui como característica a simetria das comunicações, dessa forma a velocidade adquirida no download é igual a velocidade do upload.

É oferecido por operadoras especializadas com foco no atendimento a grandes empresas que não podem sofrer com instabilidade do serviço.

É uma tecnologia utilizada por organizações cujas necessidades de comunicação são providas diretamente na Internet, sem ser preciso acessar um ambiente próprio centralizado de processamento de dados (um data center).

Principais características:

1. Qualidade da conexão;
2. Acesso mais estável, seguro, ágil e com escalabilidade elevada, eliminando o tráfego de rede;
3. Acordos de níveis de serviços, por se tratar de perfil corporativo; e

4. A disponibilidade de uso de endereços IPs (públicos e fixos) que são alocados exclusivamente para a rede da organização.

8.5. Internet Satélite

A internet via satélite funciona por meio de antenas que fazem a comunicação com satélites que possuem uma distância de 36.000 (trinta e seis mil) quilômetros da terra, o fluxo de conexão se torna mais lento visto que a distância reflete diretamente na latência dos links. Trata-se de uma solução com custo mais elevado, quando em relação a um link com as mesmas características terrestre.

Se trata de internet com limitações, onde as taxas de download são de no máximo 25 Mbps, o tempo de resposta é mais lento e pode oscilar e perder desempenho, devido as condições do tempo e adversidades.

Mesmo com as limitações, a internet satélite tem se tornado essencial para localidade remotas, cujo não há infraestrutura terrestre disponível e indisponibilidade de outros recursos tecnológicos. Dessa forma em determinadas localidades, essa pode ser a única opção de conexão com a internet. **Essa realidade não se aplica às unidades da Funasa, que estão localizadas nas capitais e outros municípios, no caso das unidades descentralizadas.**

8.6. Clear Channel - Lan-to-Lan

É um serviço de comunicação de dados, voz e imagem entre dois Clear Channel (lan-to-lan) pontos de rede que proporciona segurança, conectividade e alta qualidade. É uma solução de interconexão de redes que tem garantia de 100% da conexão, possui baixa latência e grande capacidade de largura de banda.

Sua alta performance propicia a troca e replicação de grandes volumes de informações em tempo real entre os data centers remotos, permitindo dessa forma, que a banda de internet de uso comum fique livre para as demais operações diárias.

Os grandes benefícios incluem:

1. Confiabilidade;
2. Transparência;
3. Segurança;
4. Escalabilidade;
5. Garantia de Banda;
6. Baixa latência; e
7. Alta capacidade de transferência de dados.

No caso da solução da Funasa, suas características atendem à necessidade de conexão do site central com a SUEST-GO, para replicação do ambiente de backup.

8.7. Solução de Next Generation Firewall (NGFW)

O NGFW (Next Generation Firewall) é a evolução das soluções de firewall comumente utilizadas pelas empresas, que fazem somente controle de IP de origem, IP de destino, porta de origem, porta de destino e flags de protocolo. Ele consiste num firewall de inspeção profunda de pacotes que vai além da inspeção de porta/protocolo e bloqueio para adicionar inspeção em nível de aplicativo, prevenção de invasões e traz inteligência de fora do firewall.

O NGFW foi projetado para resolver ameaças cibernéticas avançadas no nível do aplicativo. Para isso, conta com recursos de segurança capazes de reconhecer contexto e inteligência, possibilitando analisar se um download contém algum tipo de ameaça,
como ransomware, backdoor, ou outro malware, conhecido (que já tenha uma assinatura) ou desconhecido (zero day).

Ele agrega ainda funções que enxergam dentro dos pacotes de rede se existe alguma tentativa de explorar vulnerabilidades nos serviços que estão rodando na infraestrutura da empresa.

Como a Funasa já conta atualmente com uma solução Firewall NGFW, contratada em 2020, com suporte técnico e garantia vigentes até o final de 2025, os equipamentos dessa natureza não serão incluídos na presente contratação. Apesar disso, a equipe de planejamento cogitou um cenário em que essa solução atuasse como uma camada de proteção adicional. Contudo, esse cenário mostrou-se inviável no momento.

Segundo pesquisa de mercado e considerando as soluções tecnológicas existentes, os serviços de tecnologia da informação, transmissão e recepção de dados - modo bidirecional, que permita o tráfego de informações de caráter corporativo entre localidades a nível nacional simultaneamente, acesso à rede mundial de computadores (Internet), de segurança de acesso e dados e monitoramento, que atendam a necessidade da Fundação, podem ser contratados de diferentes formas:

Cenário	Descrição da solução (ou cenário)
1	Contratação de serviços de comunicação de dados com a utilização de tecnologia SD-WAN em links de Internet Banda larga e Internet dedicada
2	Contratação de serviços de comunicação de dados com internet dedicada, links MPLS, e Lan to Lan (clear channel).
3	Aquisição e implantação rede de comunicação de dados própria.

Tabela 1 - Identificação das soluções

É imperioso mencionar que as análises da equipe de planejamento priorizaram o uso de tecnologias similares à solução atualmente contratada, considerando a reduzida equipe de servidores, que além da instrução da contratação em tela, atuam em outras demandas da Coordenação-Geral de Modernização e Tecnologia da Informação - CGMTI, além do exíguo prazo para conclusão desse processo. Dadas outras circunstâncias, o escopo do estudo, com análise de outras tecnologias poderia ser ampliado.

9. Descrição da solução como um todo

A solução escolhida é o **Cenário 2 - Contratação de serviços de comunicação de dados com Internet dedicada, fornecimento de link MPLS e Lan-to-Lan,** para a execução pelo período de 12 meses.

Dessa forma, será realizada a contratação de solução integrada de tecnologia da informação, consistindo em serviços de transmissão e recepção de dados - modo bidirecional, que permita o tráfego simultâneo de informações de caráter corporativo entre localidades em âmbito nacional, compreendendo: acesso à rede mundial de computadores (Internet dedicada e compartilhada), serviço de segurança de acesso; proteção contra ataques "DDoS" para o site central, proteção de dados e monitoramento dos serviços prestados, incluindo todos os equipamentos e implementos necessários à entrega da solução.

A empresa contratada será responsável por fornecer todos os circuitos, prover o acesso à internet, dispor de solução de segurança e todos os demais insumos necessários ao perfeito funcionamento da solução de TIC.

Cabe destacar aqui, que a solução a ser contratada não está limitada, tão e somente, na entrega de circuitos de transmissão de dados, este serviço constitui a implantação, manutenção e sustentação de toda uma infraestrutura de rede de dados, serviços de acesso e monitoramento da qualidade e da segurança cibernética. Uma rede Corporativa de comunicação de dados que integra todas as unidades administrativas da Funasa, em âmbito nacional.

Devemos destacar ainda o aspecto do suporte que se faz necessário às unidades administrativas e operacionais da Funasa, estabelecimentos situados nas capitais e unidades descentralizadas, e sem os recursos de pessoal adequados a operação das tecnologias de informação e comunicações, motivo pelo qual os serviços de suporte, administração, monitoramento e segurança são tão necessários e devem estar agregados, intrínsecos aos serviços de comunicação de dados.

Os circuitos foram categorizados em C1, C2, C3.1, C3.2 e C4:

Grupo	Item	Categoria	Velocidade	Descrição	CATSER	Unidade	Qu
1	1	C1	1 Gbps	Internet Corporativo – Nó Central – Dupla Abordagem com segurança	26506	UNIDADE	1
	2	C2	1 Gbps	MPLS – Nó Central – Dupla Abordagem	26506	UNIDADE	1
	3	C3.1	100 Mbps	MPLS - Link Corporativo - SUEST	26506	UNIDADE	26
	4	C3.2	40 Mbps	MPLS - Link Corporativo - Unidades Descentralizadas	26506	UNIDADE	17
	5	C4	1 Gbps	Lan-to-Lan - SUEST GO	26506	UNIDADE	1

Tabela 2 - Solução de TIC a ser contratada

9.1. Da vigência

O contrato terá vigência de 12 (doze) meses, prorrogável para até 10 anos, na forma dos artigos 106 e 107 da Lei nº 14.133, de 2021.

9.2. Justificativa Técnica da Escolha da Solução

Ao examinar os cenários analisados, em relação ao objetivo proposto, levou-se em consideração que os serviços em utilização na contratação atual ainda fornecem os benefícios esperados pela instituição.

O posicionamento da equipe de planejamento da contratação está embasado na premissa de que a solução atual atende a necessidade da Fundação, e que o aumento das velocidades contratadas pode promover maior agilidade nos acessos ao serviços disponibilizados pelo site central.

Assim justifica-se a utilização das tecnologias MPLS e Internet Dedicada, e o link Lan-to-Lan, dada a capilaridade da instituição, para atendimento a todas as unidades administrativas, entregando serviços de dados, informação e comunicação com a melhor qualidade que cada localidade oferece, ainda no qual foi traçado estratégias de níveis de serviço para o melhor atendimento de acordo com a necessidade.

Além disso, durante a realização dos estudos para a presente contratação, a equipe de planejamento considerou diferentes cenários, com a inclusão ou não de equipamento Firewall-NGFW, nos item C1, C3.1 e C3.2, e da tecnologia SD-WAN.

A Fundação já dispõe de uma solução de Firewall NGFW, contratada em 2020, e o novo modelo de arquitetura proposto inicialmente, utilizaria essa solução de Firewall, como uma camada adicional de proteção.

Contudo, não foi possível comprovar a vantajosidade econômica desse novo modelo, como já manifestado nesse estudo. Dessa forma, a equipe de planejamento optou pela utilização da solução de Firewall já existente, e quando da sua renovação, a CGMTI poderá avaliar os cenários mais vantajosos para sua manutenção.

A contratação de soluções especializadas na modalidade serviço foi escolhida porque, além de atender às necessidades técnicas elencadas pela Funasa e também é amplamente adotada no mercado.

9.3. Benefícios técnicos a serem alcançados com a solução escolhida quanto à:

Quanto a a solução escolhida possibilitará o acesso da Funasa à rede mundial de computadores eficácia tanto para os serviços acessados pela população quanto a navegação dos servidores e colaboradores da Fundação.

Quanto a eficiência a solução escolhida possibilitará o atendimento das necessidades da instituição com uma menor utilização de mão de obra especializada em administração de ambientes computacionais.

Quanto a efetividade a solução escolhida possibilitará a disponibilidade e acesso seguro dos serviços e colaboradores da Funasa à Internet.

Quanto a economicidade escolhida possibilitará um menor uso de mão de obra especializada de servidores e colaboradores terceirizados, bem como diminuirá o risco de perda de dados críticos de acesso indevido a informações sigilosas ou restritas.

9.4. Justificativa Econômica da Escolha da Solução

Registra-se que a cotação de preços foi realizada utilizando-se diferentes composições para a contratação, com a inclusão ou não de equipamento Firewall-NGFW, nos itens C1, C3.1 e C3.2, ou sua inclusão apenas nos itens C3.1 e C3.2.

Contudo, como manifestado anteriormente, a ausência de cotações, com preços para essas composições prejudicou a comparação entres diferentes soluções.

Desse modo, a equipe optou pelo cenário mais simples e similar à solução atual. Sugerindo que, quando da renovação da solução de Firewall NGFW, a Fundação possa reavaliar a solução aqui especificada.

Reforça o entendimento da equipe de planejamento, o exíguo prazo para contratação, que não permitiria nova solicitação de cotação, ou ainda o estudo de outros cenários tecnicamente possíveis.

Nesse sentido, o **Cenário 2 - Contratação de serviços de comunicação de dados com Internet dedicada, links MPLS, e Lan to Lan (clear channel)**, sem a inclusão de equipamento Firewall NGFW, nos itens C1, C3.1 e C3.2 é a solução escolhida, do ponto de vista econômico também.

10. Estimativa das Quantidades a serem Contratadas

Do contrato atual

A Fundação Nacional de Saúde possui hoje link de internet central com a velocidade de 600 MB e um link MPLS com velocidade de 350 MB que é compartilhado com as superintendências e unidades descentralizadas.

Com a crescente utilização da Internet e do consumo do link de MPLS, com disponibilização de serviços de TI tanto para o público interno quanto externo a Fundação Nacional de Saúde, entende-se que esta velocidade CONTRATADA deverá aumentar ao longo do tempo para suprir estas necessidades.

Com objetivo de proporcionar modelo de contratação contemplando uma solução de contingenciamento para os links das unidades regionais de forma a minimizar os riscos de indisponibilidades dos serviços, foram incluídos links de internet de 20 MB para quatro unidades regionais SUEST, quais sejam: PA, PE, RJ e PR, que ao longo da execução do contrato foram desativados.

Para o link MPLS a contratação prevista era 350 MB centralizado, 20 MB para as Superintendências e 10 MB para as unidades descentralizadas.

Das dificuldades do contrato atual

O contrato nº 50/2018, responsável pela prestação desses serviços atualmente, encerra-se em 10/07/2024, e não tem possibilidade prorrogação.

Além disso, para conformidade com o Programa de Privacidade e Segurança da Informação - PPSI, é necessário agregar tecnologias não disponíveis na solução atualmente contratada.

Outrossim, a velocidade contratada, especialmente nas Superintendências Estaduais, considerando o período anterior à extinção da Funasa, que contava com um número significativamente maior de servidores e colaboradores, era insuficiente, gerando gargalos e lentidão, impactando nos trabalhos desenvolvidos pelos técnicos dessas unidades, e como demonstrado nos gráficos abaixo:

Apesar de não contar ainda, com mesmo quadro de servidores e colaboradores, há expectativa do retorno de grande parte dos servidores lotados em outros órgãos, assim como o restabelecimento dos contratos que envolvem mão de obra alocada nas dependências da Funasa, sobretudo nas SUEST, em que esses contratos perderam vigência, durante o período em que a Fundação encontrava-se extinta. Soma-se a isso, um número cada vez maior de reuniões on-line, assim como a utilização de serviços em nuvem, como por exemplo, o Office 365.

Da nova contratação

De modo a subsidiar a nova contratação, foi realizado levantamento junto às Superintendências Estaduais, para definição dos quantitativos e localidades necessárias, para instalação dos pontos de conexão, considerando as unidades das SUEST nas capitais e as unidades descentralizadas.

Desse modo, foi estabelecido o quantitativo de 26 Superintendências Estaduais e 17 unidades descentralizadas, que estão detalhados no Anexo XI – LOCAIS DE INSTALAÇÃO.

Nesse sentido, foram especificados os seguintes itens para composição da solução a ser contratada:

- Link C1: responsável pela saída e entrada de internet estruturantes do Site Central do DF;
- Link C2: interligação da rede restrita da Funasa;
- Link C3: Os links do tipo C3, serão responsáveis pelo atendimento das Superintendências Estaduais - SUEST, e das unidades descentralizadas. Considerando que as velocidades a serem contratadas serão diferentes, eles foram divididos em subcategorias: C3.1 - SUEST, e C3.2 - unidades descentralizadas;
- Link C4: Interligação entre a Funasa Presidência e a SUEST / GO, para redundância do ambiente de backup.

Como já manifestado, considerando potencial aumento no número atual de usuários, com o retorno de servidores, e a realização de contratações de serviços administrativos, a Funasa necessitará de uma expansão dos links, pois o contrato atual apresentava um quantitativo elevado de utilização dos serviços, anteriormente à publicação da Medida Provisória nº 1156/2023. Desse modo, foi realizado um cálculo estimado para ampliação do link baseado no consumo atual dos serviços já disponibilizados e previstos para os próximos anos:

Velocidade do Link	VOIP por ramal	Vídeo padrão	Aplicações, acesso remoto, Internet, e-mail e outros	Gerência da rede	Banda total alocada
40960 Kbps	30 Kbps	256 Kbps	30720 Kbps	409 Kbps	31985 Kbps
102400 Kbps	30 Kbps	256 Kbps	76800 Kbps	1024 Kbps	79684 Kbps

Tabela 4 - Links MPLS

Link de 40960 Kbps	
VOIP 20 ramais x 30k =	600
Vídeo Conferência 5 usuário x 256k =	1260
Aplicações, e-mail e outros 75% de 40960k =	30720
Gerência de rede 1% 40960k =	409

Total de utilização da banda em KBPS =	**32989**

Tabela 5 - Links MPLS - unidades descentralizadas

Link de 102400 Kbps	
VOIP 20 ramais x 30k	600
Vídeo Conferência 5 usuário x 256k	1260
Aplicações, e-mail e outros 75% de 102400k	76800
Gerência de rede 1% 102400k	1024
Total de utilização da banda em KBPS	**79684**

Tabela 6 - Links MPLS - SUEST

Fórmula de cálculo para link de rede MPLS e Internet

Somatório total dos links das unidades regionais (SUEST) multiplicado pela velocidade desses links, considerando 60% do total da operação.

26 SUEST X 102400 Kbps X 60% = 1.597.440 Kbps aproximadamente

Considerando que os acessos não são simultâneos, entende-se que o link de 1 GB atende à necessidade de conexão das SUEST e unidades descentralizadas.

MPLS: 1Gb

Internet: 1Gb

Lan-to-Lan: 1Gb

Reestruturação organizacional

No que concerne a instalação dos links nas Superintendências Estaduais e unidades descentralizadas, foram consideradas as estruturas existentes previamente à extinção da Funasa, efetivada com a publicação da Medida Provisória nº 1.156/2023.

Em que pese a caducidade da referida MP, e a consequente recriação da autarquia, até o presente, o processo de reestruturação não fora concluído.

Há a expectativa de publicação de decreto, por parte do Governo Federal, para definição tanto das atribuições e responsabilidades da instituição, como de sua estrutura organizacional.

Nesse sentido, a depender da nova estrutura, pode haver modificações que envolvam as SUEST e unidades descentralizadas, que estão contempladas nos itens C3.1 e C3.2. Além do link Lan-to-lan, a ser instalado na SUEST / GO (item C4).

Por esse motivo, a contratação prevê a possibilidade de instalação de links mediante a emissão de ordens de serviço. Além da desativação de links, após formalização da Contratante.

Tal flexibilidade, promoverá, durante a execução contratual, o ajuste dos links conforme a necessidade da instituição.

Cumpre informar, que apesar de possuir um número menor de servidores e colaboradores, atualmente, as instalações das Superintendências Estaduais continuam em funcionamento.

Categoria	**Descrição**	**Quantidade**	**Banda necessária**	**Banda a co**
C1	Internet Corporativo – Nó Central – Dupla Abordagem com segurança	1		1 Gbps
C2	MPLS – Nó Central – Dupla Abordagem	1		1 Gbps
C3.1	MPLS - Link Corporativo - SUEST	26		100 Mbps
C3.2	MPLS - Link Corporativo - Unidades Descentralizadas	17		40 Mbps
C4	Lan-to-Lan - SUEST GO	1		1 Gbps

Tabela 7 - Dimensionamento da velocidade a ser contratada

Diante do cenário apresentado, os serviços a serem objeto da nova contratação serão compostos da seguinte forma:

Grupo	**Item**	**Categoria**	**Velocidade**	**Descrição**	**CATSER**	**Unidade**	**Q M**
1	1	C1	1 Gbps	Internet Corporativo – Nó Central – Dupla Abordagem com segurança	26506	UNIDADE	1
	3	C2	1 Gbps	MPLS – Nó Central – Dupla Abordagem	26506	UNIDADE	1
	4	C3.1	100 Mbps	MPLS - Link Corporativo - SUEST	26506	UNIDADE	26
	5	C3.2	40 Mbps	MPLS - Link Corporativo - Unidades Descentralizadas	26506	UNIDADE	17
	6	C4	1 Gbps	Lan-to-Lan - Suest GO	20506	UNIDADE	1

Tabela 8 - Bens e serviços da contratação

A instalação dos links se dará na sede da Funasa em Brasília, nas Superintendências Estaduais, nas capitais, e nas unidades descentralizadas. Os endereços estão descritos no Anexo XI – LOCAIS DE INSTALAÇÃO.

11. Estimativa do Valor da Contratação

Valor total estimado: **R$ 2.301.887,46 (dois milhões, trezentos e um mil, oitocentos e oitenta e sete reais e quarenta e seis centavos).**

Grupo	Item	Descrição	Quantidade	Valor Unitário	Valor Mensa
1	1	C1 - Internet Corporativo – Nó Central – Dupla Abordagem com segurança - 1 Gbps	1	R$ 6.787,00	R$ 6.787,00
	2	C2 - MPLS – Nó Central – Dupla Abordagem - 1 Gbps	1	R$ 4.637,50	R$ 4.637,50
	3	C3.1 - MPLS - Link Corporativo - SUEST - 100 Mbps	26	R$ 3.930,00	R$ 102.180,0
	4	C3.2 - MPLS - Link Corporativo - Unidades Descentralizadas - 40 Mbps	17	R$ 2.998,28	R$ 50.970,76
	5	C4 - Lan-to-Lan - Suest GO - 1 Gbps	1	R$ 27.248,70	R$ 27.248,70
Custo mensal estimado					**R$ 191.823,9**
Custo total estimado					**R$ 2.301.887**

Tabela 9 - Estimativa de custos da contratação

12. Justificativa para o Parcelamento ou não da Solução

A equipe de planejamento da contratação avaliou que a melhor opção para o caso concreto é a manutenção de um único grupo englobando os itens do objeto.

A justificativa para o não parcelamento dar-se-á em função do nítido inter-relacionamento entre os itens distintos. A não observância desta peculiaridade sujeitaria a Administração Pública a riscos desnecessários de descontinuidade, uma vez que se veria obrigada a coordenar ações de diferentes fornecedores, com possibilidade de ocorrência de sobreposição de responsabilidades técnicas entre os mesmos dado o alto grau de integração e dependência entre as atividades desempenhadas pelos profissionais. A opção pelo não parcelamento da solução visa assegurar a harmonia durante a prestação do serviço sem implicar em maior custo de fiscalização, sendo, portanto, compatível com a capacidade de fiscalização contratual do CONTRATANTE.

A decisão de realizar ou não o parcelamento passa necessariamente pela análise dos prejuízos que podem advir da pulverização excessiva da execução de um determinado objeto pelas mais diversas pessoas, seja sob o ponto de vista da gestão como do ponto de vista da perda de economia de escala.

O CONTRATANTE já realiza suas contratações de serviços de TI procurando segmentá-las de acordo com a natureza dos serviços prestados. Fracionar ainda mais essa contratação – que, vale relembrar, tem um objeto único –, significaria dificuldades de gestão dos contratos e perda de economia de escala. Vale lembrar, nesse sentido, jurisprudência do Tribunal de Contas da

União sobre o caso:

> *"Na forma do art. 23, §1o, da Lei no 8.666/93, deve a Administração buscar o parcelamento do objeto, com vistas a melhor aproveitar os recursos do mercado e, sobretudo, ampliar a competitividade do certame. Todavia, essa orientação exige que o parcelamento somente seja efetuado quando não resultar em perda de economia de escala. Não se pode esquecer, e nisso andou bem o legislador, que a licitação é procedimento administrativo que visa, entre outros aspectos, a que a Administração contrate da forma mais vantajosa possível. Logo, não seria razoável, além de ser ilegal, que o parcelamento venha a ocasionar perda de economia de escala e, por via de consequência, maiores custos para a Administração Pública." (Decisão no 348/1999, Plenário, rel. Min. Benjamin Zymler).*

O parcelamento das contratações de serviços de TI por parte da Fundação é feito em conformidade com o poder discricionário da Administração Pública, que lhe dá a prerrogativa de fazê-lo até o limite da coerência, da viabilidade técnica e da capacidade interna de gestão.

Portanto, levando-se em consideração os aspectos técnicos, econômicos e a jurisprudência vigente, essa contratação foi agrupada em um lote único, que se entende ser a maneira mais vantajosa para execução de seu objeto.

13. Contratações Correlatas e/ou Interdependentes

Não se aplica.

14. Alinhamento entre a Contratação e o Planejamento

A contratação deste serviço está alinhada com o Plano Diretor de Tecnologia da Informação – PDTI 2022 (Sei nº 3807064) e proposta orçamentária de 2024.

Cumpre informar que as metas e ações do PDTIC 2022 foram remanejadas para o exercício atual, por meio da Portaria nº 1.554, de 26 de dezembro de 2023 (Sei nº 4683317), dado o cenário institucional de reestruturação da FUNASA.

Informamos ainda que está em processo de elaboração o Plano Diretor de TIC para o exercício de 2024, e que a ação "adquirir / manter solução de transmissão de dados, voz e vídeo" será mantida nesse planejamento, pois é essencial para a manutenção da infraestrutura, bem como para o adequado funcionamento da autarquia.

ID	META	ID	AÇÃO
M1	Implantar solução tecnológica para videoconferência e trabalho remoto na Presidência e nas Superintendências, disponibilizando equipamentos para transmissão de dados, voz e vídeo.	A1.3	Adquirir/Manter solução de transmissão de dados, voz e vídeo nas unidades da Funasa.

Tabela 10 - Alinhamento com o PDTIC

A Rede Corporativa da FUNASA disponibiliza infraestrutura física e lógica para que todos os serviços, possam ser utilizados, de forma padronizada, em todos os pontos remotos da autarquia.

Nesse sentido, a contratação desses serviços, contribui para o alcance da missão instituição da Fundação, pois além de proporcionar a integração entre a Presidência da Funasa, Superintendências Estaduais e unidades descentralizadas, provê a conexão com sistemas externos, incluindo os sistemas estruturantes do Governo Federal, como: SIAFI, SIOP, TransfereGOV,

responsáveis pela gestão orçamentária, financeira e de instrumentos de repasse (convênios e termos de compromisso), por meio dos quais a Fundação promove saúde pública e inclusão social por meio de ações de saneamento e saúde ambiental, para prevenção e controle de doenças.

Por conseguinte, a contratação está prevista no Plano anual de Contratações - PAC 2024. Além disso, os serviços prestados através dessa contratação também estão relacionados aos objetivos pactuados no Plano Pluri Anual - PPA:

Programa 2322 - Saneamento Básico	
Objetivo Geral:	Ampliar o acesso e melhorar a qualidade das ações e dos serviços de saneamento básico nas áreas urbanas e rurais, visando a universalização e a integração entre as políticas públicas relacionadas, segundo os princípios da equidade, integralidade e sustentabilidade.
Objetivos Estratégicos:	**Ampliar as capacidades de prevenção, gestão de riscos e resposta a desastres e adaptação às mudanças climáticas.** Incentivar a transição para cidades criativas e sustentáveis, com investimentos integrados em mobilidade, habitação, saneamento básico, equipamentos sociais e infraestrutura. **Promover a ampliação e o contínuo aperfeiçoamento das capacidades estatais com o fim de prestar serviços públicos de qualidade para a população, com o fortalecimento da cooperação federativa, para maior coesão nacional.**
Programa 5121 - Gestão, Trabalho, Educação e Transformação Digital na Saúde	
Objetivo Geral	Aprimorar o cuidado à saúde, fortalecendo a gestão estratégica do SUS, do trabalho e da educação em saúde, e intensificar a incorporação da inovação e da saúde digital e o enfrentamento das discriminações e desigualdades de raça/etnia, de gênero, regionais e sociais.
Objetivos Específicos	**Ampliar a democracia participativa, a transparência e o controle social.** Ampliar a qualidade dos ensinos médio, técnico e superior, preparando cidadãos e cidadãs para lidar com os desafios profissionais e éticos em um mundo em intensa transformação tecnológica. Ampliar o acesso da população à saúde pública de qualidade por meio do fortalecimento do Sistema Único de Saúde. Ampliar o desenvolvimento da ciência, tecnologia e inovação para o fortalecimento do Sistema Nacional de CT&I, a cooperação Estadoinstitutos de pesquisa-empresas e a cooperação internacional para superação de desafios tecnológicos e ampliação da capacidade. Assegurar proteção previdenciária a todas as formas de ocupação, de emprego e de relações de trabalho, com sustentabilidade financeira. **Intensificar a transformação digital nos três níveis de governo para ampliar a agilidade e a capacidade de entrega de resultados à população.** Promover a ampliação e o contínuo aperfeiçoamento das capacidades estatais com o fim de prestar serviços públicos de qualidade para a população, com o fortalecimento da cooperação federativa, para maior coesão nacional; Promover a cooperação internacional e o desenvolvimento regional integrado.

	Promover a transformação digital da economia, a inclusão digital e a disseminação da Internet de alta velocidade. Reforçar políticas de proteção e atenção às mulheres, buscando a equidade de direitos, a autonomia financeira, a isonomia salarial e a redução da violência
Programa 5123 - Vigilância em Saúde e Ambiente	
Objetivo Geral	Reduzir e controlar doenças e agravos passíveis de prevenção e controle, com enfoque na superação das desigualdades de acesso, regionais, sociais, de raça/etnia e gênero.
Objetivos Específicos	Ampliar as capacidades de prevenção, gestão de riscos e resposta a desastres e adaptação às mudanças climáticas. **Ampliar o acesso da população à saúde pública de qualidade por meio do fortalecimento do Sistema Único de Saúde.**

Tabela 11 - Alinhamento com o PPA

A presente contratação contará ainda com melhorias que agregarão maior segurança ao ambiente computacional da Funasa. Dessa forma, também contribuirá para a implementação de controles e medidas do Programa de Privacidade e Segurança da Informação - PPSI, instituído pela SGD / MGI, através da Portaria SGD/MGI nº 852/2023:

3. Controle de Cibersegurança		
Controle	**Descrição**	**Observação**
3.4. Configuração Segura de Ativos Institucionais e Software	Estabelecer e manter a configuração segura de ativos institucionais (dispositivos de usuário final, incluindo portáteis e móveis; dispositivos de rede; dispositivos não computacionais/IoT; e servidores) e software (sistemas operacionais e aplicações).	Determinadas configurações de hardware e software podem afetar negativamente a privacidade dos funcionários. Portanto, é necessária uma revisão de privacidade nas definições de configuração para garantir que determinados produtos não armazenem ou transmitam, intencionalmente ou não, dados pessoais de funcionários. A configuração dos equipamentos que compõem o serviço contratado devem estar alinhadas ao nível se segurança necessário para proteção dos dados da instituição.
3.8. Gestão de Registros de Auditoria	Coletar, alertar, analisar e reter logs de eventos com o objetivo de ajudar a detectar, compreender ou se recuperar de um ataque.	A coleta e análise de log são procedimentos críticos para que uma organização possa detectar atividades maliciosas rapidamente. Em certas ocasiões, os registros de auditoria são a única evidência de um ataque bem-sucedido. Caso os processos de análise de log sejam insatisfatórios ou inexistentes, os atacantes às vezes, podem controlar as máquinas das vítimas por meses ou anos sem que sejam percebidos pela organização-alvo.
	Estabeleça, implemente e gerencie ativamente (rastreie, reporte, corrija)	A infraestrutura de rede segura é uma defesa essencial contra os ataques. Isso inclui uma arquitetura de segurança apropriada, abordando vulnerabilidades que são, muitas vezes, introduzidas com configurações padrão, monitoramento de alterações e

3.12. Gestão da Infraestrutura de Rede	os dispositivos de rede, a fim de evitar que atacantes explorem serviços de rede e pontos de acesso vulneráveis.	reavaliação das configurações atuais. Neste caso, a segurança da rede deve estar em constante mudança, o que exige uma reavaliação regular dos diagramas de arquitetura, configurações, controles de acesso e fluxos de tráfego permitidos, de forma a evitar que os atacantes tirem proveito das configurações de dispositivos de rede que se tornam menos seguras com o tempo.
3.13. Monitoramento e Defesa da Rede	Implementar processos e ferramentas para que a organização estabeleça o monitoramento e a defesa de rede contra ameaças de segurança em toda a sua infraestrutura de rede e base de usuários.	As ferramentas de segurança somente são eficazes se oferecerem suporte a um processo de monitoramento contínuo que permita à equipe ser alertada e responder rapidamente a incidentes de segurança. Ter uma consciência situacional abrangente aumenta a velocidade de detecção e resposta, que é fundamental para minimizar um possível impacto negativo para o órgão, por exemplo, ao responder rapidamente quando um malware é descoberto, credenciais são roubadas ou quando dados sensíveis são comprometidos.
3.15. Gestão de Provedor de Serviços	Com o objetivo de garantir a proteção das informações, sistemas e processos críticos da organização, estabeleça um processo para avaliar os provedores de serviços que operem e mantenham estes ativos da organização.	Violações de terceiros costumam impactar significativamente uma organização, como por exemplo os ataques de ransomware que podem ser realizados indiretamente, quando há um bloqueio de um de seus provedores de serviço, causando a interrupção nos negócios, ou diretamente, criptografando os dados da organização. A maioria das regulamentações de segurança, privacidade e proteção de dados exigem que sua proteção seja estendida a prestadores de serviços terceirizados. A confiança de terceiros é uma função central de Governança, Riscos e Compliance (GRC), pois os riscos que não são gerenciados dentro da organização são transferidos para entidades fora da organização.
3.17. Gestão de Resposta a Incidentes	Proteger as informações e a reputação da organização, desenvolvendo e implementando uma infraestrutura de resposta a incidentes (por exemplo: planos, definição de papéis, treinamento, comunicações, gerenciamento de supervisão) para descobrir um ataque de forma ágil, e depois, conter efetivamente o impacto, eliminar a presença do atacante, e restaurar a integridade da rede e dos sistemas da organização.	O objetivo principal da resposta a incidentes é identificar ameaças na organização, responder a elas antes que possam se espalhar e remediá-las antes que possam causar danos.

Tabela 12 - Alinhamento com o PPSI

15. Análise Comparativa de Soluções

A Instrução Normativa SGD/ME nº 94 de 23 de novembro de 2023, estabelece no art. 11, II, que para a análise comparativa de soluções, devem ser considerados, além do aspecto econômico, os aspectos qualitativos em termos de benefícios para o alcance dos objetivos da contratação. Essa análise deverá observar o seguinte:

> *(...)*
> *a) necessidades similares em outros órgãos ou entidades da Administração Pública e as soluções adotadas;*
> *b) as alternativas do mercado;*
> *c) a existência de softwares disponíveis conforme descrito na Portaria STI/MP nº 46, de 28 de setembro*

de 2016;
d) as políticas, os modelos e os padrões de governo, a exemplo dos Padrões de Interoperabilidade de Governo Eletrônico - ePing, Modelo de Acessibilidade em Governo Eletrônico - eMag, Padrões Web em Governo Eletrônico - ePwg, Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil e Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos - e-ARQ Brasil, quando aplicáveis;
e) as necessidades de adequação do ambiente do órgão ou entidade para viabilizar a execução contratual;
f) os diferentes modelos de prestação do serviço;
g) os diferentes tipos de soluções em termos de especificação, composição ou características dos bens e serviços integrantes;
h) a possibilidade de aquisição na forma de bens ou contratação como serviço; e
i) a ampliação ou substituição da solução implantada;
j) as diferentes métricas de prestação do serviço e de pagamento.

Neste sentido, para composição desse estudo técnico, foi realizada a análise dos cenários possíveis para a realização da contratação ora pretendida, como forma de evidenciar as diferentes formas de prestação de serviços e escolha de solução mais vantajosa para a Funasa.

Os cenários definidos pela equipe de planejamento da contratação tem como objetivo a Contratação de solução integrada de tecnologia da informação, consistindo em serviços de transmissão e recepção de dados - modo bidirecional que permita o tráfego simultâneo de informações de caráter corporativo entre localidades em âmbito nacional, acesso à rede mundial de computadores (Internet), serviço de segurança de acesso, proteção de dados e monitoramento dos serviços prestados, incluindo todos os equipamentos e implementos necessários à entrega da solução.

Necessidades similares em outros órgãos ou entidades da Administração Pública e as soluções adotadas

Foram identificadas contratações cujo objeto tem alguma similaridade a contratação pretendida pelo Funasa, conforme tabela abaixo:

Órgão / Entidade	**Identificação do Pregão**	**Objeto**	**Solução adotada**
SENAC	041/2022	Registro de preços para a eventual contratação de serviços de telecomunicações (link dedicado de internet, serviços de rede VPN/MPLS e internet via satélite), conforme especificações do edital e seus anexos	Link MPLS, e internet dedicada
Conselho Federal Representantes Comerciais	002/2023	CANAL DE COMUNICAÇÃO (LINK) DE INTERNET DEDICADA com no mínimo 5 (cinco) IP´s fixos válidos. Rede de comunicação de dados na modalidade IP MPLS + DDoS Item 2 Internet ADSL	Link MPLS, e internet dedicada
Justiça Federal	044/2022	Contratação de serviços de telecomunicações necessários à implantação, operação, manutenção e gerenciamento de uma Rede IP Multisserviços, por meio da tecnologia MPLS, objetivando a interligação da rede corporativa de longa distância (WAN) das 4 (quatro) Subseções Judiciárias do Maranhão ao prédio sede da Seccional em São Luís pelo período de 30 (trinta) meses, conforme Termo de Referência	Link MPLS
	027/2022	Solução integrada de tecnologia da informação, consistindo em serviços de transmissão e recepção de dados - modo bidirecional, que permita o tráfego simultâneo de informações de caráter corporativo entre localidades em âmbito nacional, compreendendo: acesso à rede mundial de computadores (Internet dedicada e compartilhada); serviço de segurança de acesso; proteção contra	Link MPLS, internet dedicada, DDos,

Ministério da Saúde		ataques "DDoS" para os sites centrais; proteção dedados e monitoramento dos serviços prestados, incluindo todos os equipamentos e implementos necessários à entrega da solução, conforme especificações deste Termo de Referência.	equipamentos e monitoramento
Polícia Federal	018/2023	Contratação de empresas especializadas na prestação de serviços MPLS com instalação, configuração, suporte e manutenção corretiva de enlaces de comunicação, incluindo ainda fornecimento de equipamentos (com suporte e substituição em campo) necessários para uma solução integrada de rede de longa distância que suporte as demandas da Polícia Federal.	Link MPLS

Tabela 13 - Contratações similares na Administração Pública

Várias outras contratações, no âmbito da Administração Pública, que guardam similaridade com a contratação em tela foram identificadas e analisadas pela equipe de planejamento, quando da análise de preços, nos termos da Nota Técnica nº 7/2024 /CGMTI/DEADM/PRESI (Sei nº 4755132).

- **As alternativas do mercado**
  - Para os cenários 1 e 2, as alternativas de mercado correspondem à um modelo padronizado executado por empresas de Telecom, qual seja a disponibilização dos links, fornecimento de hardware, software, serviços de instalação dos meios físicos e lógicos e sua manutenção, a fim de assegurar o fornecimento constante e contínuo, de alta qualidade e disponibilidade, de forma ininterrupta.
  - Com relação ao cenário 3, seria necessário a contratação de todos os requisitos informados acima e ainda a contratação de empresas para implantação da rede em âmbito nacional, aquisição de equipamentos, contratação de empresa para implementação dos equipamentos, incluindo suporte e manutenção e contratação de empresa para gerência e sustentação de toda a rede.

- **A existência de software público brasileiro, quando aplicável**
  - Não se aplica. A presente contratação não se trata apenas da contratação de software.

- **As políticas, os modelos e os padrões de governo, a exemplo do ePing, eMag, ePwg, ICP-Brasil e e-ARQ Brasil, quando aplicáveis**
  - Sim, as soluções tecnológicas são aderentes ao e-Ping principalmente aos seguimentos 1 (interconexão) e 2 (segurança).

- **As necessidades de adequação do ambiente do órgão ou entidade para viabilizar a execução contratual (exemplo: mobiliário, instalação elétrica, espaço adequado para prestação do serviço, etc.)**
  - Não é necessária adequação do ambiente do órgão para a execução contratual para os cenários 1 e 2.
  - Sobre o cenário 3, será necessário realizar adequações que deverão ser previstas no Projeto Implementação em virtude da necessidade de criação de toda a infraestrutura para conexão de dados.

- **Diferentes modelos de prestação do serviço**
  - Os diferentes modelos de tráfego de dados são os descritos no levantamento de soluções item 8 (Levantamento de mercado) deste estudo.

- **Diferentes tipos de soluções em termos de especificação, composição ou características dos bens e serviços integrantes**

- Com relação aos cenários de 1 e 2, a empresa que prestará os serviços de transmissão e recepção de dados poderia oferecer diferentes tipos de composição dos serviços, dependendo da necessidade de cada cliente, observando apenas a disponibilidade para cada localidade, de acordo com as seguintes composições:

    1. Tipos de conexão: fibra, cabo, satélite, etc.
    2. Tipo de tecnologia: MPLS, SD-WAN, internet banda larga, internet dedicada, internet móvel, etc.
    3. Velocidade dos links;
    4. Fornecimento de equipamentos: Roteadores, Firewalls, anti-DDoS e SD-WAN, etc.; e
    5. Serviços de implantação e monitoramento.

- No que refere ao cenário 4, a contratação seria realizada de forma separada para compor a infraestrutura de comunicação de dados para atender à autarquia, necessitando da contratação de empresa especializada para elaboração de projeto executivo de redes de comunicação em âmbito nacional, contratação de empresa especializada para fornecimento e implementação de rede de comunicação, aquisição de equipamentos, contratação de serviços para implementação dos equipamentos e manutenção da rede, contratação de serviços de internet, além da contratação de equipe técnica especializada para o gerenciamento, manutenção, sustentação e administração da rede.

- **A possibilidade de aquisição na forma de bens ou contratação como serviço**
    - Referente aos cenários 1 e 2, ocorreria mediante contratação como serviço desonerando a autarquia da necessidade de aquisição de equipamentos.
    - Com relação ao cenário 3, a contratação ocorreria tanto na forma de bens, como serviço.

- **A ampliação ou substituição da solução implantada**
    - A presente contratação visa substituir o contrato administrativo nº 50/2018, que terá sua vigência expirada em 10 /07/2024, sem possibilidade de prorrogação.
    - Desse modo, não é possível a ampliação da solução implantada atualmente.

- **Outros aspectos comparativos**

Requisito	**Solução**	**Sim**	**Não**	**Não se aplica**
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Cenário 1	x		
	Cenário 2	x		
	Cenário 3		x	
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Cenário 1			x
	Cenário 2			x
	Cenário 3			x
A Solução é composta por software livre ou software público? (quando se tratar de software)	Cenário 1			x
	Cenário 2			x
	Cenário 3			x

A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Cenário 1	x		
	Cenário 2	x		
	Cenário 3	x		
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Cenário 1			x
	Cenário 2			x
	Cenário 3			x
funcionais do e-ARQ Brasil? (quando o objetivo da solução abrangerA Solução é aderente às orientações, premissas e especificações técnicas e documentos arquivísticos)	Cenário 1			x
	Cenário 2			x
	Cenário 3			x

Tabela 14 - Aspectos comparativos

15.1. Conclusão - Cenário 1 - Contratação de serviços de comunicação de dados com a utilização de tecnologia SD-WAN em links de Internet Banda larga e Internet dedicada

Trata-se de contratação de serviços de comunicação de dados com a utilização de tecnologia SD-WAN em links de Internet Banda larga e Internet dedicada, as principais vantagens da utilização da tecnologia SDWAN são a possibilidade de formação de túneis isolados para o acesso seguro de uma ponta a outra, manter a integridade dos dados e informações, a largura de banda pode ser adicionada ou reduzida conforme necessidade, implementar políticas de rede baseadas em gerenciamento centralizado, fornecer gerenciamento e segurança (firewall incluso) na saída Internet local, direcionar o tráfego baseado em políticas por aplicação e aplicar o uso inteligente de links com monitoração dinâmica de desempenho e falha. Destaca-se que todos os ambientes do grupo I poderiam utilizar a tecnologia SD-WAN, o que garante o aumento das camadas de segurança no acesso aos sistemas e informações hospedados nos ambientes físicos e lógicos do MS.

Para a implementação da tecnologia SD-WAN é necessário a utilização de links de internet sejam dedicados ou banda larga, os quais devem estar de acordo com as necessidades de cada ambiente quanto à velocidade e capacidade de transmissão e recepção de dados e informações. Para a composição da Rede Funasa, os links do grupo I devem ser interconectados aos nós centrais, dessa forma há a necessidade de implementação de camadas de segurança, as quais devem ser providas pelo uso de novas tecnologias, como por exemplo a SD-WAN.

A utilização de tal tecnologia visa garantir que as operações sejam realizadas de forma exclusiva sem que haja interferências externas causando riscos e possíveis vulnerabilidades, o que pode acarretar em indisponibilidade, perda e vazamento de informações corporativas.

Ainda nesse contexto cabe destacar que, em situações específicas o tempo de latência do link SD-WAN se torna maior do que o tempo de latência do link MPLS. O atendimento das Superintendências Estaduais, e a sede da Funasa, em Brasília, além da SUEST - GO seriam melhores atendidos com o uso de links de tecnologia MPLS, garantindo alto nível velocidade, segurança, disponibilidade, integridade, rede de uso exclusivo e tempo de resposta preciso de acordo com a necessidade da operação.

Sendo assim **concluímos que, a contratação de serviços de comunicação de dados com a utilização de tecnologia SD-WAN em links de Internet Banda larga e Internet dedicada, não é a melhor solução para a Fundação, no momento, do ponto de vista da latência quando comparado com a tecnologia MPLS** desejável para os links de categoria C2, C3.1 e C3.2.

15.2. Conclusão - Cenário 2 - Contratação de serviços de comunicação de dados com internet dedicada, links MPLS, e Lan to Lan (clear channel).

Trata-se de contratação de serviços de comunicação de dados com fornecimento de internet dedicada, link MPLS, e Lan to Lan (clear channel). Esse cenário, que possui maior similaridade com a solução atual, atende às necessidades de conectividade entre as unidades da Funasa, incluindo a Sede em Brasília, as Superintendências Estaduais localizadas nas capitais e as unidades descentralizadas.

O link Clear Channel (lan-to-lan) promoverá a interligação entre o data center em Brasília e o ambiente de redundância de backup instalado na SUEST / GO.

Considerando o momento de reestruturação da instituição e a reduzida força de trabalho da CGMTI, além do fato de que a solução atual atende à necessidade da instituição, a equipe de planejamento da contratação, optou pela utilização desta solução, destacando a melhor configuração ofertada no que for possível, para o atendimento de todas as localidades, conforme topologia abaixo:

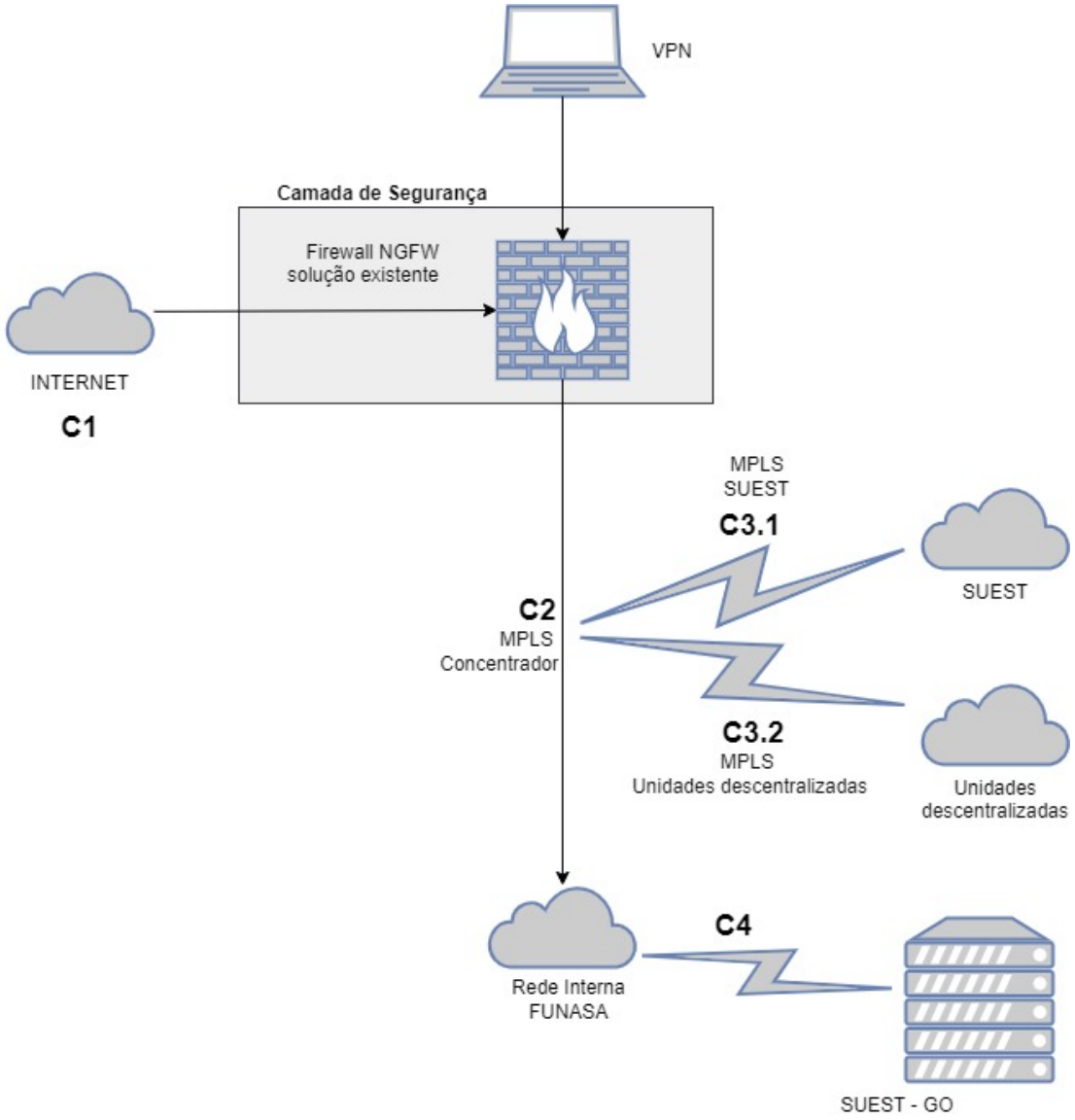

Figura 1 - Topologia Rede Funasa

Em face dos argumentos apresentados acima, **a equipe de planejamento da contratação conclui que este cenário (contratação de serviços de comunicação de dados com internet dedicada, links MPLS, e Lan to Lan), atende na totalidade do projeto**

da Rede Funasa e se torna viável, por apresentar alta disponibilidade e um bom custo benefício, já que é composto por tecnologias consolidadas no mercado e adequadas para ambientes corporativos com tráfego de informações críticas.

15.3. Conclusão - Cenário 3 - Aquisição e implantação rede de comunicação de dados própria.

Trata-se de aquisição e implantação de rede de comunicação de dados própria, para esse cenário é necessária a contratação de empresa especializada para a elaboração de Projeto Executivo de Redes de Comunicação em âmbito nacional, contratação de empresa especializada para fornecimento e implementação de rede de comunicação, aquisição de equipamentos, contratação de serviços para implementação dos equipamentos e manutenção da rede, contratação de serviços de internet e contratação de equipe técnica especializada para o gerenciamento, manutenção, sustentação e administração da rede. Tendo em vista, a complexidade para a implementação de infraestrutura de comunicação de dados própria e o grande volume de contratos que demandam a construção.

Ademais, investimentos prévios da prestadora de serviço impactam diretamente no projeto, tal como disponibilidade de link MPLS na região. As soluções oferecidas pelas empresas também impactariam diretamente nos equipamentos, já que há a possibilidade de as empresas apresentarem soluções compostas de roteador e firewall em um único equipamento ou não, o que impactaria diretamente nos projetos e nos quantitativos.

Ainda por se tratar de um cenário complexo, há a necessidade de um estudo aprofundado na verificação da viabilidade técnica e financeira, o que leva tempo para a construção do projeto executivo, visto que se trata de redes a serem implementadas em âmbito nacional e que cada quilômetro deve ser mapeado, para o indicativo de uma infraestrutura segura e eficiente, dos pontos estratégicos de conexões, dos materiais e insumos necessários, dos equipamentos mais adequados para a implementação da rede, do esforço empregado e do Custo Total de Propriedade. Leva-se em consideração também a quantidade de contratos que demandaria este modelo de contratação, o que torna inviável no ponto de vista da gerência das redes, gestão de SLA e gestão de contratos, dada a quantidade reduzida de servidores que atuam na CGMTI.

15.4. Registro de Soluções Consideradas Inviáveis

Por todo o exposto no item que trata da “ANÁLISE COMPARATIVA DE SOLUÇÕES”, o cenário 1 de forma isolada foi considerado inviável, devido ao tempo de latência do link SD-WAN, em situações específicas, que se torna maior do que o tempo de latência do link MPLS.

Referente ao cenário 3, destaca-se que, em virtude da amplitude das redes, as tecnologias necessárias e o grau de complexidade, a execução nos moldes desse cenário torna-se inviável, considerando inclusive a força de trabalho da Fundação, notadamente a que se dedica a gestão dos recursos de TI, o cenário não é viável para a contratação desses serviços.

Cenário	Cenários inviáveis
1	Contratação de serviços de comunicação de dados com a utilização de tecnologia SD-WAN em links de Internet Banda larga e Internet dedicada
3	Aquisição e implantação de rede de comunicação de dados própria

Tabela 15 - Soluções inviáveis

16. ANÁLISE COMPARATIVA DE CUSTOS (TCO)

Cálculo dos custos totais de propriedade

Para elaboração do custo total de propriedade, a solução viável identificada nesse Estudo Técnico Preliminar, é o **Cenário 2 - Contratação de serviços de comunicação de dados com Internet dedicada, links MPLS, e Lan to Lan (clear channel)**.

Conforme determinado na Instrução Normativa SGD/ME nº 94 de 23 de dezembro de 2023, deverá ser realizada a análise comparativa de custos envolvidos na contratação. Para isso, deverão ser consideradas somente as soluções viáveis, bastando o registro das soluções inviáveis no Estudo Técnico Preliminar da Contratação:

> *(...)*
>
> *Art.11*
>
> *(...)*
>
> *III - A análise comparativa de custos deverá considerar apenas as soluções técnica e funcionalmente viáveis, incluindo:*
>
> *a) cálculo dos custos totais de propriedade (Total Cost Ownership - TCO) por meio da obtenção dos custos inerentes ao ciclo de vida dos bens e serviços de cada solução, a exemplo dos valores de aquisição dos ativos, insumos, garantia técnica estendida, manutenção, migração e treinamento; e*
>
> *b) memória de cálculo que referencie os preços e os custos utilizados na análise, com vistas a permitir a verificação da origem dos dados;*

Solução Viável - Contratação de serviços de comunicação de dados com link de internet dedicada, links MPLS e Lan to Lan (clear channel)

Grupo	Item	Categoria	Velocidade	Descrição	CATSER	Unidade	Qua M
1	1	C1	1 Gbps	Internet Corporativo – Nó Central – Dupla Abordagem com segurança	26506	UNIDADE	1
	2	C2	1 Gbps	MPLS – Nó Central – Dupla Abordagem	26506	UNIDADE	1
	3	C3.1	100 Mbps	MPLS - Link Corporativo - SUEST	26506	UNIDADE	26
	4	C3.2	40 Mbps	MPLS - Link Corporativo - Unidades Descentralizadas	26506	UNIDADE	17
	5	C4	1 Gbps	Lan-to-Lan - SUEST GO	26506	UNIDADE	1

Tabela 16 - Itens que compõe a solução

Conforme determinado pela Instrução Normativa SEGES/ME nº 73, de 5 de agosto de 2020, a metodologia para obtenção dos preços estimados poderá ser realizada da seguinte forma:

> *"Art. 5º A pesquisa de preços para fins de determinação do preço estimado em processo licitatório para a aquisição e contratação de serviços em geral será realizada mediante a utilização dos seguintes parâmetros, empregados de forma combinada ou não:*

> *I - Painel de Preços, disponível no endereço eletrônico gov.br/painel de preços, desde que as cotações refiram-se a aquisições ou contratações firmadas no período de até 1 (um) ano anterior à data de divulgação do instrumento convocatório;*
>
> *II - aquisições e contratações similares de outros entes públicos, firmadas no período de até 1 (um) ano anterior à data de divulgação do instrumento convocatório;*
>
> *III - dados de pesquisa publicada em mídia especializada, de sítios eletrônicos especializados ou de domínio amplo, desde que atualizados no momento da pesquisa e compreendidos no intervalo de até 6 (seis) meses de antecedência da data de divulgação do instrumento convocatório, contendo a data e hora de acesso; ou*
>
> *IV - pesquisa direta com fornecedores, mediante solicitação formal de cotação, desde que os orçamentos considerados estejam compreendidos no intervalo de até 6 (seis) meses de antecedência da data de divulgação do instrumento convocatório.*
>
> ***§1º Deverão ser priorizados os parâmetros estabelecidos nos incisos I e II**." (grifo nosso)*

A pesquisa foi realizada junto ao Painel de Preços do Ministério da Gestão, conforme registro da equipe de planejamento da contratação, nos termos da Nota Técnica nº 7/2024/CGMTI/DEADM/PRESI (Sei nº 4755132), no que tange ao inciso I, do art. 5º Instrução Normativa nº 73, de 5 de agosto de 2020. Porém, os resultados foram limitados, para cada item, mesmo ampliando a pesquisa no Comprasnet e analisando várias contratações similares. Isso se deu devido as características técnicas das soluções encontradas, que quando comparadas às características do objeto desejado, possuem diferenciais, que podem ser em relação às tecnologias, velocidades diferentes, agrupamentos de itens, ou desmembramento de serviços de segurança dissociados dos itens de conexão.

Assim, os preços utilizados para estimativa do valor utilizaram-se da combinação entre os incisos I, II e IV, do art. 5º Instrução Normativa nº 73, de 5 de agosto de 2020, como detalhado na Nota Técnica nº 7/2024.

O pedido de cotação, junto aos fornecedores, solicitou apresentação de preço para diferentes composições, para subsidiar a comparação da equipe de planejamento, em busca da solução mais vantajosa:

- Composição 1: Inclui fornecimento, instalação e configuração de 2 equipamentos Cluster Firewall – NG, nos itens 1, 3 e 4;
- Composição 2: Inclui fornecimento, instalação e configuração de 2 equipamentos Cluster Firewall – NG, nos itens 3 e 4. O item 1 utiliza solução Firewall NGFW existente;
- Composição 3: Não prevê fornecimento de equipamentos Cluster Firewall – NG, para os itens 1, 3 e 4.

Para cada composição, deveriam ser ofertados valores para vigência de 12 e 60 meses.

Entretanto, somente duas empresas responderam à solicitação, e não possuíam os elementos necessários para um comparativo adequado.

Nesse sentido, não havendo meios de realizar a análise de vantajosidade do ponto de vista econômico, para as diferentes composições inicialmente cogitadas, a equipe de planejamento optou por realizar a contratação da solução equivalente à atual, aumentando as velocidades dos links, para suportar de forma adequada os serviços agregados desde a contratação de 2018, como o Office 365, além de sustentar de forma satisfatória, eventual aumento no consumo em virtude do aumento de conexões VPN, de servidores que por ventura estão atuando, ou ainda atuarão de forma remota (integral ou parcialmente), quando da adesão ao Programa de Gestão por Demandas - PGD.

Em relação ao prazo da contratação, dado que não pôde ser avaliada eventual diferença de valores para a contratação de 12 e 60 meses, a equipe entendeu como viável a manutenção do prazo de 12 meses, considerando também, que a solução de de Firewall, adquirida pela Funasa previamente, tem garantia até 12/2025, e quando dos estudos para sua renovação, a instituição pode reavaliar a vantajosidade de inclusão da solução nos serviços de conexão.

Itens	**Composição 1**		**Composição 2**		**Composição 3**	

-	**Valor para 12 meses**	**Valor para 60 meses**	**Valor para 12 meses**	**Valor para 60 meses**	**Valor para 12 meses**	**Valo mese**
Item 1 - C1: Internet corporativo	Não houve cotação para a composição, com prazo de vigência de 12 meses	Não houve cotação para a composição, com prazo de vigência de 60 meses	Não houve cotação para a composição, com prazo de vigência de 12 meses	Não houve cotação para a composição, com prazo de vigência de 60 meses	R$ 81.444,00	
Item 2 - C2: MPLS - Nó central					R$ 55.650,00	
Item 3 - C3.1: MPLS - SUEST					R$ 1.226.160,00	Não h cotaç comp prazo de 60
Item 4 - C3.2 - MPLS - Unidades descentralizadas					R$ 611.649,12	
Item 5 - C4 - Lan-to-Lan - SUEST - GO					R$ 326.984,40	
Valor anual estimado	-	-	-	-	**R$ 2.301.887,52**	-

Tabela 17 - Análise comparativa

17. Providências a serem Adotadas

Não será necessária nenhuma adequação ao ambiente da Funasa para viabilizar a execução contratual, visto que a contratação trata-se de prestação de serviço de TIC e a área gestora comumente fiscaliza contratos similares ao que será celebrado a partir deste processo.

18. Resultados Pretendidos

Dentre os diversos benefícios observados na presente contratação, que estão relacionados a princípios como eficiência, eficácia e efetividade, destacam-se:

- Assegurar a continuidade da prestação do serviço de acesso à Internet com capacidade suficiente para atendimento às demandas previstas pela Funasa, com vistas à atender aos requisitos de segurança da informação e comunicações da Fundação.
- Prover o acesso à Internet e atendimento ao público interno, convenentes e compromitentes, órgãos de controle e à sociedade em geral.
- Promover o acesso às informações e serviços junto à autarquia, além do acesso aos demais órgãos da Administração Pública Federal;

- Suportar o funcionamento dos processos de negócio e servidores públicos das unidades descentralizadas da Funasa, no tocante ao acesso à Internet;
- Aumentar o nível de segurança e disponibilidade das informações trafegadas entre as unidades da Fundação.

19. Possíveis Impactos Ambientais

A contratada deverá fornecer, no ato da assinatura do contrato, o Plano de Gerenciamento de Resíduos Sólidos ou Declaração de Sustentabilidade Ambiental, comprovando a correta destinação dos cartuchos/toners usados e o pleno atendimento à legislação vigente. No caso da logística reversa, a empresa contratada deve apresentar semestralmente (no máximo),declaração confirmando o recebimento dos cartuchos e toners já utilizados e respectivas embalagens dos equipamentos, para fins de reaproveitamento no ciclo produtivo das próprias empresas, em outros ciclos (como cooperativas de reciclagem) ou outra destinação final ambientalmente adequada. A periodicidade desse recolhimento deverá ser mensal, de forma a não deixar acumular os materiais utilizados sem serventia nas dependências do IFMA.

Os equipamentos fornecidos deverão possuir funcionalidades que promovam a economia de energia elétrica, como, por exemplo, modo de economia de energia.

Além disso, deverá adotar boas práticas de otimização de recursos/redução de desperdícios/ menor poluição, quando couber. tais como:
a) Racionalização do uso de substâncias potencialmente tóxico poluentes;
b) Substituição de substâncias tóxicas por outras atóxicas ou de menor toxicidade;
c) Adotar as práticas de sustentabilidade na execução dos serviços, todas de acordo com o art. 6º da Instrução Normativa SLTI /MPOG nº 1, de 19 de janeiro de 2010 e Decreto nº 10.024, de 20 de setembro de 2019.

20. Declaração de Viabilidade

Esta equipe de planejamento declara **viável** esta contratação.

20.1. Justificativa da Viabilidade

O presente planejamento foi elaborado em harmonia com a Instrução Normativa SGD/ME nº 94/2022, bem como em conformidade com os requisitos técnicos necessários ao cumprimento das necessidades e objeto da contratação.

O presente planejamento está em conformidade com os requisitos administrativos necessários ao cumprimento do objeto e está de acordo com as necessidades técnicas, operacionais e estratégicas do órgão.

Esta solução é, do ponto de vista técnico-econômico, a mais vantajosa para a Administração Pública, já que atenderá perfeitamente às necessidades da Funasa, os níveis de serviços desejados e com a melhoria na performance das redes de comunicação de dados. Ainda que, dos possíveis cenários é a única que contempla as soluções tecnológicas necessárias e disponíveis para atendimento do projeto em sua totalidade.

O presente estudo técnico preliminar visa a Contratação de solução integrada de tecnologia da informação, consistindo em serviços de transmissão e recepção de dados - modo bidirecional que permita o tráfego simultâneo de informações de caráter corporativo entre localidades em âmbito nacional, acesso à rede mundial de computadores (Internet), serviço de segurança de acesso, proteção de dados e monitoramento dos serviços prestados, incluindo todos os equipamentos e implementos necessários à entrega da solução.

Finalmente, a proposta apresentada nesse estudo visa atender e atualizar as capacidades das redes de comunicação de dados da Fundação em âmbito nacional, buscando fornecer serviços com qualidade, proteção e performance para as demandas em saúde, juntamente com suporte, garantia e níveis de serviços que permitam o funcionamento ininterrupto de toda a Rede Funasa.

Com base nas informações levantadas ao longo do estudos técnico preliminar, bem como no histórico do Contrato nº 50/2018, a equipe de planejamento declara que a contratação é viável e, do ponto de vista técnico, é essencial para os trabalhos realizados pela autarquia.

21. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

SERGIO LUIZ DE CASTRO

Integrante técnico

Assinou eletronicamente em 25/06/2024 às 17:51:53.

RAQUEL MARRA MOLINA DE AGUIAR

Integrante requisitante

Assinou eletronicamente em 25/06/2024 às 17:37:17.

Lista de Anexos

Atenção: Apenas arquivos nos formatos ".pdf", ".txt", ".jpg", ".jpeg", ".gif" e ".png" enumerados abaixo são anexados diretamente a este documento.

- Anexo I - Anexo I - Modelo planilha custos e formação de preços.pdf (418.6 KB)
- Anexo II - Anexo II - Niveis minimos de servico.pdf (1006.72 KB)
- Anexo III - Anexo III - Termo de Sigilo.pdf (671.28 KB)
- Anexo IV - Anexo IV - Termo de Ciencia.pdf (583.31 KB)
- Anexo V - Anexo V - Ordem de serviço.pdf (605.9 KB)
- Anexo VI - Anexo VI - TRP.pdf (597.92 KB)
- Anexo VII - Anexo VII - TRD.pdf (583.17 KB)
- Anexo VIII - Anexo VIII - Termo de encerramento contrato.pdf (598.05 KB)
- Anexo IX - Anexo IX - Requisitos técnicos para prestação do serviço.pdf (850.9 KB)
- Anexo X - Anexo X - Arquitetura da Rede Funasa.pdf (911.57 KB)
- Anexo XI - Anexo XI - Locais de Instalação.pdf (738.34 KB)

Anexo I - Anexo I - Modelo planilha custos e formação de preços.pdf

Anexo I - Modelo Planilha de Preços

CONTRATAÇÃO DE SERVIÇO DE ACESSO À INTERNET

Discriminação dos Serviços (dados referentes à contratação)	
Razão Social	
CNPJ	
Endereço Completo	
Tels. Contato (com DD)	
E-mail contato	
Responsável pela Proposta	

PROPOSTA DE PREÇO

Grupo	Item	Categoria	Descrição	CATSER	Velocidade	Unidade	Quantidade Mensal	Valor Unitário	Valor Total
1	1	C1	Internet Corporativa - Nó Central - dupla Abordagem com segurança	26506	1 Gbps	Unidade	1	R$	R$
	3	C2	MPLS - Nó central - Dupla Abordagem	26506	1 Gbps	Unidade	1	R$	R$
	4	C3.1	MPLS - Link Corporativo - SUEST	26506	100 Gbps	Unidade	26	R$	R$
	5	C3.2	MPLS - Link Corporativo - Unidades Descentralizadas	26506	40 Mbps	Unidade	17	R$	R$
	6	C4	Lan-to-Lan - Suest GO	26506	1 Gbps	Unidade	1	R$	R$
Valor Global								**R$**	**R$**

[Cidade]/[UF], [dia] de [mês] de [ano].

_____

[Assinatura do Responsável pela Proposta]
RESPONSÁVEL PELA PROPOSTA (NOME COMPLETO)
CARGO DO RESPONSÁVEL PELA PROPOSTA

Anexo II - Anexo II - Niveis minimos de servico.pdf

Anexo II – NÍVEIS MÍNIMOS DE SERVIÇO

SUMÁRIO

1. Níveis Mínimos de Serviços

1.1. O Nível de Serviço Contratado (NSC) estabelece valores limites aceitáveis para o bom desempenho dos serviços contratados e serão descritos a seguir. Serão adotados os indicadores de níveis de serviço de disponibilidade e de tempo de reparo. O não cumprimento desses indicadores sujeita a CONTRATADA aos descontos descritos nesta seção;

1.2. Mensalmente os demonstrativos de Nível de Serviço deverão ser apresentados para a Funasa, incluindo informações sobre ações e necessidades para a correção e desvios, visando atingir, manter e melhorar os níveis alcançados;

1.3. Os demonstrativos de Nível de Serviço, a pedido da CONTRATANTE, poderão ser adaptados quanto ao formato e ao nível de detalhamento conforme as necessidades identificadas pela Funasa durante a vigência do contrato;

1.4. Todos os circuitos deverão ser fornecidos com banda garantida. Entende-se por banda garantida o valor efetivo de banda entregue à Funasa, considerando o *overhead* da tecnologia utilizada;

1.5. A CONTRATADA deverá garantir que todos os circuitos tenham, suas especificações, em conformidade com o disposto nas tabelas do subitem 8.24.3, aferidas mensalmente por meio de ferramenta disponibilizada, sem custo, pela CONTRATADA. Sem prejuízo de eventual aferição, por parte da Funasa, com utilização de ferramenta, podendo inclusive confrontar os dados apresentados pela CONTRATADA, que, em caso de desvios, deverá apresentar justificativas;

1.6. A CONTRATADA ficará desobrigada do cumprimento dos níveis de serviço enquanto a prestação destes estiver prejudicada em função de impedimento ou retardo decorrente de responsabilidade comprovada da CONTRATANTE ou casos excepcionais (fortuitos ou força maior). Fica estabelecido que em caso de divergências, a CONTRATANTE dará o posicionamento final a respeito da(s) divergência(s).

2. Metodologia de Avaliação da Qualidade

2.1. A contratada deverá cumprir os seguintes indicadores de níveis de serviços, conforme as metas especificadas adiante:

a) IDM - Disponibilidade dos serviços de Acesso à Rede;
b) IDV - Indicador de Nível de disponibilidade aceitável;
c) IVRep – Indicador do Tempo de Reparo Ponto de Presença;
d) TPDV – Indicador do Tempo de Atendimento à Incidentes e Requisições de Segurança;
e) PINL - Prazo para Implantação de Serviços novos links;
f) PACT - Prazo para Alteração de Característica Técnica (PACT);
g) PMEF - Prazo para Mudanças de Endereço Físico (PMEF);

2.2. Para melhor compreensão dos indicadores de níveis de serviço que serão apresentados como requisitos obrigatórios, segue detalhamento:

2.1.1. IDM - Indicador de Disponibilidade dos serviços de Acesso à Rede

2.1.1.1. Este indicador deve ser avaliado para cada um dos Pontos de Presença;

2.1.1.2. A disponibilidade do serviço indica o percentual de tempo, durante o período do mês de operação em questão, em que todos os serviços (todos os elementos de hardware e/ou software) deverão permanecer em condições normais de funcionamento.

Fórmula de cálculo:

IDM = [1 - (Tim - Tip) / (Tom - Tip)] x 100

onde:
IDM: índice de disponibilidade mensal do serviço de Acesso à Rede, em porcentagem (%)
Tom: período total em horas correspondente a um mês de operação, equivalente a 720 (setecentos e vinte) horas.
Tim: somatório dos tempos de indisponibilidade do serviço durante o período de operação (um mês), em horas.
Tip: somatório dos tempos de indisponibilidade referentes a interrupções programadas de responsabilidade ou aprovadas pela Funasa. Deverão ser incluídos neste índice os tempos de indisponibilidade permitidos para realização de manutenções preventivas, conforme os limites definidos a seguir: a CONTRATADA poderá se valer de até 4 (quatro) horas em cada mês, não cumulativos entre meses, para realização das manutenções preventivas, fora do horário comercial e previamente acordada com a Funasa.

2.1.2. IDV - Indicador de Nível de disponibilidade aceitável

2.1.2.1. Para todos os circuitos: Consultar Tabelas do subitem 8.24.3.

Fórmula de cálculo:

IVD= 100 – IDM

Onde:
IVD: índice mensal de violação do Indicador de Disponibilidade em porcentagem (%)

2.1.3. IVRep – Indicador do Tempo de Reparo Ponto de Presença

2.1.3.1. Refere-se ao tempo para a resolução de um problema técnico, considerando o intervalo entre a abertura do chamado (recebimento do respectivo número) e o reparo definitivo do problema, ou seja, o restabelecimento da normalidade do serviço para cada circuito.

Fórmula de cálculo:

Trep = Trepf - Trepi
IVRep = (TrepVI / 720)

onde:

Trep: Tempo de reparo aferido da solicitação em horas;

Trepf: data e hora do término do atendimento com a resolução definitiva do problema;

Trepi: data e hora da abertura do chamado;

TRM: tempo de reparo máximo aceitável para cada uma das solicitações individuais, em horas, após o reparo definitivo do problema, considerando o estabelecido nas tabelas do subitem 8.24.3, Fator 4 – Tempo de Reparo de Circuito;

TrepVI = somatório dos tempos de violação dos tempos de reparo registrados para todas as solicitações no período de operação do circuito, em horas (no mês);

TrepVI = [somatório (Trep - TRM)], somente quando Trep for maior que TRM;

IVRep: Índice mensal de violação dos Indicadores de reparo para todas as solicitações em porcentagem (%);

2.1.3.2. Ao **TRM** indicado acima, será permitido o acréscimo de 2 (duas) horas para cada 50 (cinquenta) km adicionais de distância entre o município do circuito e a capital do Estado, quando da necessidade de intervenção presencial.

2.1.4. TPDV – Indicador do Tempo de Atendimento à Incidentes e Requisições de Segurança

2.1.4.1. Refere-se ao tempo decorrido para o atendimento à incidentes ou requisições de Segurança, considerando o intervalo entre a abertura do chamado, a adoção de medida de contorno e a conclusão definitiva do chamado.

Fórmula de cálculo:

Tatsc = Tsc – Tacs
Se Tatsc > TMASC, então:
CDSC= Tatsc / ciclo;
Tatsd = Tsd – Tacs;
Se Tatsd > TMASD, então:
CDSD= Tatsd / ciclo;
TPDV = (CDSC*PDSC + CDSD*PDSD)

onde:

Tatsc: Tempo de atendimento a solução de contorno do chamado de segurança, em horas corridas após a abertura do chamado;

Tatsd: Tempo atendimento a solução definitiva do chamado de segurança, em horas corridas após a abertura do chamado;

Tsc: data e hora da solução de contorno do chamado de segurança;

Tsd: data e hora da solução definitiva do chamado de segurança;

Tacs: data e hora da abertura do chamado de segurança;

TMASC: Tempo máximo, em horas e minutos, de atendimento da solução de contorno de cada incidente ou requisição de segurança. Os **TMASC** estão

estabelecidos no subitem 7.3.2, tabelas 16-A, 16-B e 16-C, em função de sua severidade e prioridade;

TMASD: Tempo máximo, em horas e minutos, de atendimento ou solução definitiva de cada incidente ou requisição de segurança. Os **TMASD** estão estabelecidos no subitem 7.3.2, tabelas 16-A, 16-B, 16-C e 16-D, em função de sua severidade e prioridade;

Ao **TMASC e TMASD** indicados acima, será permitido o acréscimo de 2 (duas) horas para cada 50 (cinquenta) km adicionais de distância entre o município do Ponto de Presença e a capital do Estado, quando da necessidade de intervenção presencial;
PDSC = Percentual de Desconto por descumprimento do prazo para a solução de Contorno em função da severidade do incidente;
CDSD: Número de ciclos em descumprimento da solução Definitiva, estabelecidos nas tabelas 16-A, 16-B e 16-C, coluna "Percentual de Desconto por descumprimento de prazo para solução Definitiva";
Ciclo: período em horas e minutos que define o intervalo de verificação do atendimento a um incidente ou requisição, conforme definido nas tabelas 16-A, 16-B e 16-C, coluna "percentual de desconto por descumprimento";

TPDV: Total dos percentuais de descontos por descumprimento dos prazos para adoção das soluções de contorno e definitiva (violação do **TMASC e TMASD),** para cada chamado de segurança, em função de sua severidade e prioridade estabelecidas no subitem 8.25;

2.2. PINL - Prazo para Implantação de Serviços novos links:

2.2.1. Define o tempo esperado para implantação dos serviços e ativação dos links novos.

2.2.2. Prazo superior ao previsto no do TR, ensejará em sanções estabelecidas no TR.

2.3. PACT - Prazo para Alteração de Característica Técnica

2.3.1. Define o tempo esperado para alteração de características técnicas de um dado recurso. As características técnicas consideradas incluem a velocidade, estabelecimento de canais privativos e parametrização referente a classes de serviços.

2.3.2. Prazo superior ao previsto no TR, ensejará em sanções estabelecidas no TR.

2.4. PMEF - Prazo para Mudanças de Endereço Físico

2.4.1. Define o tempo esperado para transferência da instalação de um dado recurso de um endereço físico para outro, sem descontinuidade da prestação do serviço, bem como para solicitações futuras de novos links.

2.4.2. Na eventualidade de serem necessárias obras de adequação, de responsabilidade da FUNASA, que afetem a instalação do recurso no endereço de destino, a contagem do tempo será suspensa até a conclusão dessas obras.

2.4.3. Prazo superior ao previsto no TR, ensejará em sanções estabelecidas no TR.

3. Para os pagamentos mensais referentes aos links

3.1. Para fins de pagamento das mensalidades dos links, o valor dos serviços prestados será calculado com base no número de links em operação em cada mês;

3.2. Somente serão considerados em operação os links que contarem com a emissão do competente Termo de Aceitação de acordo com os procedimentos indicados;

3.3. No primeiro mês de prestação dos serviços deverão ser cobrados os dias efetivamente em operação, ou seja, do primeiro dia após a emissão do Termo de Aceite até o último dia da vigência da Ordem de Serviço;

3.4. Para os meses subsequentes a cobrança deverá ser relativa ao período integral da Ordem de Serviço; e

3.5. Serão deduzidos dos valores a serem pagos à CONTRATADA, os respectivos valores de descontos, conforme previsto nesta seção.

4. Procedimentos para Descontos:

4.1. O não cumprimento do Nível de Serviço Contratado (NSC) implicará em Descontos por Violação de Indicador (**DVI)** nas mensalidades para cada link;

4.2. A penalidade para o link será composta pelo somatório de descontos, que está limitado ao valor máximo de 100% (cem por cento) do valor da Mensalidade do circuito (MPP), sendo aplicado a todos os meses de execução do contrato em que ocorram violações;

4.3. Os descontos nas mensalidades dos serviços prestados deverão ser aplicados proporcionalmente ao índice de violação dos indicadores apresentados anteriormente no subitem 8.24.3;

4.4. Serão excluídos do cálculo, os tempos de paralisação, decorrentes dos seguintes eventos:

a) Janela de manutenção acordada entre CONTRATADA e CONTRATANTE;
b) Falhas na infraestrutura provisionada pela CONTRATANTE.

4.5. Entende-se que haverá uma fase inicial de transição e adequação dos processos de atendimento por parte da CONTRATADA. Sendo assim, os níveis de serviço contratado (NSC) não serão exigidos contratualmente durante os primeiros 90 (noventa) dias corridos de duração do contrato. Os índices deverão ser apurados e apresentados para a Funasa, no entanto, a CONTRATADA não estará sujeita a penalidades pelo seu descumprimento durante este período.

4.6. Desconto por violação do indicador de disponibilidade do serviço de acesso à rede

Fórmula de cálculo:

Para IDM (Índice de Disponibilidade Mensal) menor que o indicador de nível de disponibilidade aceitável conforme item 8.24.3 do TR, aplica-se desconto proporcional ao IVD:

DVI = [(IVD/100) x MPP] x 0,4 [em R$]

DVI – Desconto por Violação de Indicador;

IVD - Índice de Violação do Indicador de Disponibilidade;
MPP - Mensalidade do Ponto de Presença.

4.7. Desconto por violação do indicador de tempo de reparo

Fórmula de cálculo:

DVI = IVRep x MPP x 0,4 [em R$]

onde:

IVRep: Índice mensal de violação dos Indicadores de tempo de reparo para todas as solicitações em % do link.
DVI: desconto mensal em R$ a ser aplicado a cada link, referente a violação do indicador de Tempo de Reparo.
MPP: Valor unitário da mensalidade do Ponto de Presença (link).

4.7.1. O desconto DVI deverá ser calculado para cada link individualmente.

4.7.2. Os valores das mensalidades a que se referem às fórmulas correspondem aos valores vigentes para o link em questão.

4.8. Desconto por violação do indicador de tempo de atendimento a incidentes e requisições de segurança

Fórmula de cálculo:

DVI = MPP x TPDV

onde:

MPP: Valor unitário da mensalidade do Ponto de Presença (link).
TPDV: Total dos percentuais de descontos por descumprimento dos prazos para adoção da solução de contorno e solução definitiva. Estes percentuais estão estabelecidos no subitem 8.25 do TR, em função da severidade e prioridade dos chamados de segurança.
DVI: desconto mensal em R$ a ser aplicado a cada link, referente a violação do TMAS - Tempo de Atendimento a Incidentes e Requisições de Segurança. DVI corresponde à coluna TG (Total da Glosa) nas matrizes de exemplo de glosa para as tabelas citadas anteriormente.
O desconto DVI deverá ser calculado para cada link individualmente.
Os valores das mensalidades a que se referem às fórmulas correspondem aos valores vigentes para o link em questão.
Quando houver, além de descumprimento do SLA da segurança, a indisponibilidade do link, deverá ser aplicada cumulativamente a penalidade pela indisponibilidade conforme subitem 4.6.

Anexo III - Anexo III - Termo de Sigilo.pdf

TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO

INTRODUÇÃO
O Termo de Compromisso de Manutenção de Sigilo registra o comprometimento formal da Contratada em cumprir as condições estabelecidas no documento relativas ao acesso e utilização de informações sigilosas da Contratante em decorrência de relação contratual, vigente ou não. **Referência: Art. 18, Inciso V, alínea "a" da IN SGD/ME Nº 94/2022.**

Pelo presente instrumento a FUNDAÇÃO NACIONAL DE SAÚDE, sediada no SAUS, Quadra 04, Bloco N, Brasília/DF, CEP: 70.070-040, CNPJ n° 26.989.350/0001-16, doravante denominado **CONTRATANTE**, e, de outro lado, a <NOME DA EMPRESA>, sediada em <ENDEREÇO>, CNPJ n° <Nº do CNPJ>, doravante denominada **CONTRATADA**;
CONSIDERANDO que, em razão do **CONTRATO N.º <nº do contrato>** doravante denominado **CONTRATO PRINCIPAL**, a **CONTRATADA** poderá ter acesso a informações sigilosas do **CONTRATANTE**; CONSIDERANDO a necessidade de ajustar as condições de revelação destas informações sigilosas, bem como definir as regras para o seu uso e proteção; CONSIDERANDO o disposto na Política de Segurança da Informação e Privacidade da **CONTRATANTE**;
Resolvem celebrar o presente **TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO,** doravante **TERMO**, vinculado ao **CONTRATO PRINCIPAL**, mediante as seguintes cláusulas e condições abaixo discriminadas.

1 – OBJETO

Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz respeito ao trato de informações sigilosas disponibilizadas pela CONTRATANTE e a observância às normas de segurança da informação e privacidade por força dos procedimentos necessários para a execução do objeto do CONTRATO PRINCIPAL celebrado entre as partes e em acordo com o que dispõem a Lei 12.527, de 18 de novembro de 2011, Lei nº 13.709, de 14 de agosto de 2018, e os Decretos 7.724, de 16 de maio de 2012, e 7.845, de 14 de novembro de 2012, que regulamentam os procedimentos para acesso e tratamento de informação classificada em qualquer grau de sigilo.

2 – CONCEITOS E DEFINIÇÕES

Para os efeitos deste TERMO, são estabelecidos os seguintes conceitos e definições:

INFORMAÇÃO: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

INFORMAÇÃO SIGILOSA: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquela abrangida pelas demais hipóteses legais de sigilo.

CONTRATO PRINCIPAL: contrato celebrado entre as partes, ao qual este TERMO se vincula.

3 – DA INFORMAÇÃO SIGILOSA

Serão consideradas como informação sigilosa, toda e qualquer informação classificada ou não nos graus de sigilo ultrassecreto, secreto e reservado. O TERMO abrangerá toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: *know-how*, técnicas, especificações, relatórios, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de ideias, aspectos financeiros e econômicos, definições, informações sobre as atividades da CONTRATANTE e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao CONTRATO PRINCIPAL, doravante denominados INFORMAÇÕES, a que diretamente ou pelos seus empregados, a CONTRATADA venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do CONTRATO PRINCIPAL celebrado entre as partes.

4 – DOS LIMITES DO SIGILO

As obrigações constantes deste TERMO não serão aplicadas às INFORMAÇÕES que:

I – sejam comprovadamente de domínio público no momento da revelação, exceto se tal fato decorrer de ato ou omissão da CONTRATADA;

II – tenham sido comprovadas e legitimamente recebidas de terceiros, estranhos ao presente TERMO;

III – sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as partes cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

5 – DIREITOS E OBRIGAÇÕES

As partes se comprometem a não revelar, copiar, transmitir, reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do CONTRATO PRINCIPAL, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas INFORMAÇÕES, que se restringem estritamente ao cumprimento do CONTRATO PRINCIPAL.

Parágrafo Primeiro – A CONTRATADA se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento prévio e expresso da CONTRATANTE.

Parágrafo Segundo – A CONTRATADA compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do CONTRATO PRINCIPAL sobre a existência deste TERMO bem como da natureza sigilosa das informações.

I – A CONTRATADA deverá firmar acordos por escrito com seus empregados visando garantir o cumprimento de todas as disposições do presente TERMO e dará ciência à CONTRATANTE dos documentos comprobatórios.

Parágrafo Terceiro – A CONTRATADA obriga-se a tomar todas as medidas necessárias à proteção da informação sigilosa da CONTRATANTE, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pela CONTRATANTE.

Parágrafo Quarto – Cada parte permanecerá como fiel depositária das informações reveladas à outra parte em função deste TERMO.

I – Quando requeridas, as INFORMAÇÕES deverão retornar imediatamente ao proprietário, bem como todas e quaisquer cópias eventualmente existentes.

Parágrafo Quinto – A CONTRATADA obriga-se por si, sua controladora, suas controladas, coligadas, representantes, procuradores, sócios, acionistas e cotistas, por terceiros eventualmente consultados, seus empregados, contratados e subcontratados, assim como por quaisquer outras pessoas vinculadas à CONTRATADA, direta ou indiretamente, a manter sigilo, bem como a limitar a utilização das informações disponibilizadas em face da execução do CONTRATO PRINCIPAL.

Parágrafo Sexto – A CONTRATADA, na forma disposta no parágrafo primeiro, acima, também se obriga a:

I – Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das INFORMAÇÕES, no território brasileiro ou no exterior, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objetivo aqui referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o uso indevido por qualquer pessoa que, por qualquer razão, tenha acesso a elas;

II – Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmos judiciais, inclusive as despesas processuais e outras despesas derivadas, a divulgação ou utilização das INFORMAÇÕES por seus agentes, representantes ou por terceiros;

III – Comunicar à CONTRATANTE, de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das INFORMAÇÕES, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente; e

IV – Identificar as pessoas que, em nome da CONTRATADA, terão acesso às informações sigilosas.

6 – VIGÊNCIA

O presente TERMO tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de sua assinatura até expirar o prazo de classificação da informação a que a CONTRATADA teve acesso em razão do CONTRATO PRINCIPAL.

7 – PENALIDADES

A quebra do sigilo e/ou da confidencialidade das INFORMAÇÕES, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na rescisão do CONTRATO PRINCIPAL firmado entre as PARTES. Neste caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pela CONTRATANTE, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis, conforme Art. 156 da Lei nº. 14.133/2021.

8 – DISPOSIÇÕES GERAIS

Este TERMO de Confidencialidade é parte integrante e inseparável do CONTRATO PRINCIPAL.

Parágrafo Primeiro – Surgindo divergências quanto à interpretação do disposto neste instrumento, ou quanto à execução das obrigações dele decorrentes, ou constatando-se casos omissos, as partes buscarão solucionar as divergências de acordo com os princípios de boa fé, da equidade, da razoabilidade, da economicidade e da moralidade.

Parágrafo Segundo – O disposto no presente TERMO prevalecerá sempre em caso de dúvida e, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos conexos firmados entre as partes quanto ao sigilo de informações, tal como aqui definidas.

Parágrafo Terceiro – Ao assinar o presente instrumento, a CONTRATADA manifesta sua concordância no sentido de que:

I – A CONTRATANTE terá o direito de, a qualquer tempo e sob qualquer motivo, auditar e monitorar as atividades da CONTRATADA;

II – A CONTRATADA deverá disponibilizar, sempre que solicitadas formalmente pela CONTRATANTE, todas as informações requeridas pertinentes ao CONTRATO PRINCIPAL.

III – A omissão ou tolerância das partes, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo;

IV – Todas as condições, termos e obrigações ora constituídos serão regidos pela legislação e regulamentação brasileiras pertinentes;

V – O presente TERMO somente poderá ser alterado mediante TERMO aditivo firmado pelas partes;

VI – Alterações do número, natureza e quantidade das informações disponibilizadas para a CONTRATADA não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste TERMO, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;

VII – O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações, conforme definição do item 3 deste documento, disponibilizadas para a CONTRATADA, serão incorporados a este TERMO, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas, sendo necessário a formalização de TERMO aditivo ao CONTRATO PRINCIPAL;

VIII – Este TERMO não deve ser interpretado como criação ou envolvimento das Partes, ou suas filiadas, nem em obrigação de divulgar INFORMAÇÕES para a outra Parte, nem como obrigação de celebrarem qualquer outro acordo entre si.

9 – FORO

A CONTRATANTE elege o foro da <CIDADE DA CONTRATANTE>, onde está localizada a sede da CONTRATANTE, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

10 – ASSINATURAS

E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO é assinado pelas partes em 2 vias de igual teor e um só efeito.

CONTRATADA	**CONTRATANTE**
_____ <Nome> <Qualificação>	_____ <Nome> **Matrícula:** xxxxxxxx
TESTEMUNHAS	
_____ <Nome> <Qualificação>	_____ <Nome> <Qualificação>

<Local>, <dia> de <mês> de <ano>.

Anexo IV - Anexo IV - Termo de Ciencia.pdf

FUNDAÇÃO NACIONAL DE SAÚDE
Setor de Autarquias Sul (SAUS) – Quadra 4 – Bloco N, Edifício Funasa - Bairro Asa Sul, Brasília/DF, CEP 70070-040

TERMO DE CIÊNCIA

INTRODUÇÃO
O Termo de Ciência visa obter o comprometimento formal dos empregados da contratada diretamente envolvidos na contratação quanto ao conhecimento da declaração de manutenção de sigilo e das normas de segurança vigentes no Órgão/Entidade. No caso de substituição ou inclusão de empregados da contratada, o preposto deverá entregar ao Fiscal Administrativo do Contrato os Termos de Ciência assinados pelos novos empregados envolvidos na execução dos serviços contratados. **Referência: Art. 18, Inciso V, alínea "b" da IN SGD/ME Nº 94/2022.**

1 – IDENTIFICAÇÃO			
CONTRATO Nº	xxxx/aaaa		
OBJETO	<objeto do contrato>		
CONTRATADA	<nome da contratada>	**CNPJ**	xxxxxxxxxxxx
PREPOSTO	<Nome do Preposto da Contratada>		
GESTOR DO CONTRATO	<Nome do Gestor do Contrato>	**MATR.**	xxxxxxxxxxxx

2 – CIÊNCIA

Por este instrumento, os funcionários abaixo identificados declaram ter ciência e conhecer o inteiro teor do Termo de Compromisso de Manutenção de Sigilo e as normas de segurança vigentes da Contratante.

Funcionários da Contratada		
Nome	**Matrícula**	**Assinatura**
<Nome do(a) Funcionário(a)>	<xxxxxxxxxx>	
<Nome do(a) Funcionário(a)>	<xxxxxxxxxx>	
…	…	…

<Local>, <dia> de <mês> de <ano>.

Anexo V - Anexo V - Ordem de serviço.pdf

FUNDAÇÃO NACIONAL DE SAÚDE
Setor de Autarquias Sul (SAUS) Quadra 4 - Bloco N, Edificio Sede - Bairro Asa Sul, Brasília/DF, CEP 70070-040

ORDEM DE SERVIÇO OU DE FORNECIMENTO DE BENS

INTRODUÇÃO
Por intermédio da Ordem de Serviço (OS) ou Ordem de Fornecimento de Bens (OFB) será solicitado formalmente à Contratada a prestação de serviço ou o fornecimento de bens relativos ao objeto do contrato. O encaminhamento das demandas deverá ser planejado visando a garantir que os prazos para entrega final de todos os bens e serviços estejam compreendidos dentro do prazo de vigência contratual. **Referência: Art. 32 IN SGD Nº 94/2022.**

1 – IDENTIFICAÇÃO			
Nº da OS/OFB	xxxx/aaaa	**Data de emissão**	<dd/mm/aaaa>
CONTRATO/NOTA DE EMPENHO nº	xx/aaaa		
Objeto do Contrato	<Descrição do objeto do contrato>		
Contratada	<Nome da contratada>	**CNPJ**	99.999.999/9999-99
Preposto	<Nome do preposto>		
Início vigência	<dd/mm/aaaa>	**Fim vigência**	<dd/mm/aaaa>
ÁREA REQUISITANTE			
Unidade	< Sigla – Nome da unidade>		
Solicitante	<Nome do solicitante>	**E-mail**	

2 – ESPECIFICAÇÃO DOS BENS/SERVIÇOS E VOLUMES ESTIMADOS					
Item	**Descrição do bem ou serviço**	**Métrica**	**Valor unitário (R$)**	**Qtde/Vol.**	**Valor Total (R$)**
1	...	...	...	...	...
	...	...	...	...	...
Valor total estimado da OS/OFB					

3 – <INSTRUÇÕES/ESPECIFICAÇÕES> COMPLEMENTARES
<Incluir instruções complementares à execução da OS/OFB> <Ex.: Contatar a área solicitante para agendamento do horário de entrega> <Ex.: Conforme consta no Termo de Referência, o recebimento provisório está condicionado à entrega do código no ambiente de homologação, e a documentação do software no repositório oficial de gestão de projetos>

4 – DATAS E PRAZOS PREVISTOS			
Data de Início:	<dd/mm/aaaa>	**Data do Fim:**	<dd/mm/aaaa>

CRONOGRAMA DE EXECUÇÃO/ENTREGA			
Item	**Tarefa/entrega**	**Início**	**Fim**
1		<dd/mm/aaaa>	<dd/mm/aaaa>
...		<dd/mm/aaaa>	<dd/mm/aaaa>

5 – ARTEFATOS / PRODUTOS	
Fornecidos	**A serem gerados e/ou atualizados**

5 – ASSINATURA E ENCAMINHAMENTO DA DEMANDA

Autoriza-se a <execução dos serviços / entrega dos bens> correspondentes à presente <OS/OFB>, no período e nos quantitativos acima identificados.

_____	_____
<Nome >	<Nome >
<Responsável pela demanda/ Fiscal Requisitante>	**Gestor do Contrato**
Matr.: <Nº da matrícula>	Matr.: <Nº da matrícula>

<Local>, xx de xxxxxxxxx de xxxx

Anexo VI - Anexo VI - TRP.pdf

TERMO DE RECEBIMENTO PROVISÓRIO – SERVIÇOS DE TIC

INTRODUÇÃO
O Termo de Recebimento Provisório trata-se de termo detalhado que declarará que os serviços foram prestados e atendem às exigências de caráter técnico, sem prejuízo de posterior verificação de sua conformidade com as exigências contratuais, baseada nos requisitos e nos critérios de aceitação definidos no Modelo de Gestão do Contrato. **Referência: Inciso XXI, art. 2º, e alínea "i", inciso II, art. 33 da IN SGD/ME Nº 94/2022.**

1 – IDENTIFICAÇÃO			
CONTRATO Nº	xx/aaaa		
CONTRATADA	<Nome da Contratada>	**CNPJ**	xxxxxxxxxxxx
Nº DA OS	<xxxx/aaaa>		
DATA DA EMISSÃO	<dd/mm/aaaa>		

2 – ESPECIFICAÇÃO DOS SERVIÇOS E VOLUMES DE EXECUÇÃO			
SOLUÇÃO DE TIC			
<Descrição da solução de TIC solicitada relacionada ao contrato anteriormente identificado>			
ITEM	**DESCRIÇÃO DO BEM OU SERVIÇO**	**MÉTRICA**	**QUANTIDADE**
1	<Descrição igual ao da OS de abertura>	<Ex.: PF>	<n>
...	...	...	...
...	...	...	...
...	...	...	...
TOTAL DE ITENS			

3 – RECEBIMENTO

Para fins de cumprimento do disposto no art. 33, inciso II, alínea "i", da IN SGD/ME nº 94/2022, por este instrumento ATESTO que os serviços correspondentes à <OS> acima identificada, conforme definido no Modelo de Execução do contrato supracitado, foram executados e <atende(m)/atende(m) parcialmente/não atende(m)> às respectivas exigências de caráter técnico discriminadas abaixo. Não obstante, estarão sujeitos à avaliação específica para verificação do atendimento às demais exigências contratuais, de acordo com os Critérios de Aceitação previamente definidos no Modelo de Gestão do contrato.

Ressaltamos que o recebimento definitivo desses serviços ocorrerá somente após a verificação desses requisitos e das demais condições contratuais, desde que não se observem inconformidades ou divergências quanto às especificações constantes do Termo de Referência e do Contrato acima identificado que ensejem correções por parte da **CONTRATADA**. Por fim, reitera-se que o objeto poderá ser rejeitado, no todo ou em parte, quando estiver em desacordo com o contrato.

ITEM	ESPECIFICAÇÃO TÉCNICA	ATENDIMENTO	OBSERVAÇÃO
1	<exigências técnicas definidas no TR>	...	.....
...	...	...	.....
...	...	...	.....
...	...	...	.....

4 – ASSINATURA

FISCAL TÉCNICO

_____
<Nome do Fiscal Técnico do Contrato>
Matrícula: xxxxxx

<Local>, <dia> de <mês> de <ano>.

PREPOSTO
_____ <Nome do Preposto do Contrato> **Matrícula**: xxxxxx <Local>, <dia> de <mês> de <ano>.

Anexo VII - Anexo VII - TRD.pdf

FUNDAÇÃO NACIONAL DE SAÚDE
Setor de Autarquias Sul (SAUS) Quadra 4 - Bloco N, Edificio Sede - Bairro Asa Sul, Brasília/DF, CEP 70070-040

TERMO DE RECEBIMENTO DEFINITIVO

INTRODUÇÃO
O Termo de Recebimento Definitivo declarará formalmente à Contratada que os serviços prestados ou que os bens fornecidos foram devidamente avaliados e atendem às exigências contratuais, de acordo com os requisitos e critérios de aceitação estabelelcidos. **Referência: Inciso XXII, Art. 2º e alínea "h" inciso I do art. 33, da IN SGD/ME Nº 94/2022.**

1 – IDENTIFICAÇÃO			
CONTRATO/NOTA DE EMPENHO Nº	xx/aaaa		
CONTRATADA	<Nome da Contratada>	**CNPJ**	xxxxxxxxxxxx
Nº DA OS/OFB	<xxxx/aaaa>		
DATA DA EMISSÃO	<dd/mm/aaaa>		

2 – ESPECIFICAÇÃO DOS PRODUTO(S)/BEM(S)/SERVIÇOS E VOLUMES DE EXECUÇÃO				
SOLUÇÃO DE TIC				
<descrição da solução de TIC solicitada relacionada ao contrato anteriormente identificado>				
ITEM	**DESCRIÇÃO DO BEM OU SERVIÇO**	**MÉTRICA**	**QUANTIDADE**	**TOTAL**
1	<descrição igual à da OS/OFB de abertura>	<Ex.: PF>	<n>	<total>
...				
TOTAL DE ITENS				

3 – ATESTE DE RECEBIMENTO

Para fins de cumprimento do disposto no art. 33, inciso II, alínea "h", da IN SGD/ME nº 94/2022, por este instrumento ATESTO/ATESTAMOS que o(s) <serviço(s)/ bem(s)> correspondentes à <OS/OFB> acima identificada foram <prestados/entregues> pela **CONTRATADA** e ATENDEM às exigências contratuais, discriminadas abaixo, de acordo

com os Critérios de Aceitação previamente definidos no Modelo de Gestão do Contrato acima indicado.

ITEM	EXIGÊNCIA CONTRATUAL	ATENDIMENTO	OBSERVAÇÃO
1	<exigência contratual estabelecida no TR >	...	.....
...	...	...	.....
...	...	...	.....
...	...	...	.....

4 – DESCONTOS EFETUADOS E VALOR A LIQUIDAR

De acordo com os critérios de aceitação e demais termos contratuais, <não> há incidência de descontos por desatendimento dos indicadores de níveis de serviços definidos.

<Não foram / Foram> identificadas inconformidades técnicas ou de negócio que ensejam indicação de glosas e sanções, <cuja instrução corre em processo administrativo próprio (nº do processo)>.

Por conseguinte, o valor a liquidar correspondente à <OS/OFB> acima identificada monta em R$ <valor> (<valor por extenso>).

Referência: <Relatório de Fiscalização nº xxxx ou Nota Técnica nº yyyy>.

5 – ASSINATURA

GESTOR DO CONTRATO

_____

<Nome do Gestor do Contrato>
Matrícula: xxxxxxxx

<Local>, <dia> de <mês> de <ano>.

<As seções seguintes podem constar em documento diverso, pois dizem respeito à autorização para o faturamento, a cargo do Gestor do Contrato, e a respectiva ciência do preposto quanto a esta autorização>.

5 – AUTORIZAÇÃO PARA FATURAMENTO
GESTOR DO CONTRATO
Nos termos da alínea "n", inciso I, art. 33, da IN SGD/ME nº 94/2022, AUTORIZA-SE a **CONTRATADA** a <faturar os serviços executados / apresentar as notas fiscais dos bens entregues> relativos à supracitada <OS/OFB>, no valor discriminado no item 4, acima. _____ <Nome do Gestor do Contrato> **Matrícula:** xxxxxxxx <Local>, <dia> de <mês> de <ano>

7 – CIÊNCIA
PREPOSTO
_____ <Nome do Preposto do Contrato> **Matrícula**: xxxxxxx <Local>, <dia> de <mês> de <ano>

Anexo VIII - Anexo VIII - Termo de encerramento contrato.pdf

FUNDAÇÃO NACIONAL DE SAÚDE
Setor de Autarquias Sul (SAUS) – Quadra 4 – Bloco N, Edifício Funasa - Bairro Asa Sul, Brasília/DF, CEP 70070-040

TERMO DE ENCERRAMENTO DO CONTRATO

INTRODUÇÃO
O Termo de Encerramento do Contrato encerrará formalmente o pacto contratual entre a Contratante e a Contratada. **Referência: Art. 35 IN SGD/ME Nº 1/2019.**

1 – IDENTIFICAÇÃO			
CONTRATO Nº	<xxxxx/aaaa>		
GESTOR DO CONTRATO	<Nome do Gestor do Contrato>		
CONTRATADA	<Nome da Contratada>	**CNPJ**	<XX.XXX.XXX/XXXXX-XX>
DATA DE INÍCIO	<dd/mm/aaaa>		
OBJETO	<Descrição do Objeto>		

2 – LISTA DE VERIFICAÇÃO			
Item	**Atendido**	**Não Atendido**	**Não Aplicável**
Os recursos humanos e materiais foram preparados para a continuidade do negócio por parte da Administração?			
A contratada entregou as versões finais dos produtos e a documentação?			
Houve a transferência final de conhecimentos sobre a execução e manutenção da solução?			
A contratada devolveu os recursos que foram oferecidos para operacionalizar o contrato?			
Foram revogados os perfis de acesso dos funcionários da contratada?			
Foram eliminadas as caixas postais que foram oferecidas à contratada?			
<outras que se apliquem ao objeto da contratação>			
...			

< É importante considerar o período de garantia, que pode se estender para além da vigência do contrato. Nestes casos, deve-se verificar quais recursos devem ser mantidos à empresa para que ela preste o serviço de garantia>.

3 – DO ENCERRAMENTO

Por este instrumento, as partes acima identificadas resolvem registrar o encerramento do contrato em epígrafe e ressaltar o que segue:

O contrato encerra-se por motivo de <motivo>.

As partes concedem-se mutuamente plena, geral, irrestrita e irrevogável quitação de todas as obrigações diretas e indiretas decorrentes deste contrato, não restando mais nada a reclamar de parte a parte.

Não estão abrangidas pela quitação ora lançada e podem ser objeto de exigência ou responsabilização mesmo após o encerramento do vínculo contratual:

a) As obrigações relacionadas a processos iniciados de penalização contratual;

b) As garantias sobre bens e serviços entregues ou prestados, tanto legais quanto convencionais;

c) A reclamação de qualquer tipo sobre defeitos ocultos nos produtos ou serviços entregues ou prestados.

d) <inserir pendências, se houver>.

E assim tendo lido e concordado com todos seus termos, firmam as partes o presente instrumento para que surta seus efeitos jurídicos.

6 – ASSINATURAS

_____ **CONTRATADA** Preposto	_____ **CONTRATANTE** <Autoridade Competente da Área Administrativa>
_____ <Nome> **Matrícula:** xxxxxxxxx	_____ <Nome> **Matrícula:** xxxxxxxxx

<Local>, <dd> de <mês> de <ano>.

Anexo IX - Anexo IX - Requisitos técnicos para prestação do serviço.pdf

Anexo IX - REQUISITOS TÉCNICOS DA PRESTAÇÃO DOS SERVIÇOS

Sumário

1. Serviços

1.1. Serviço de Instalação e Configuração

1.1.1. Faz parte da prestação do serviço, além da porta de interconexão a Internet global de forma dedicada, o transporte do sinal da CONTRATADA até as instalações do Funasa, ou seja, com a instalação de cabos, *modems*, *switches*, *racks*, fibras óticas e/ou rádios necessários a prestação do serviço.

1.1.2. A instalação do ponto de acesso físico na Funasa é de responsabilidade exclusiva da CONTRATADA.

1.1.3. A CONTRATADA deverá fornecer toda a infraestrutura necessária para disponibilizar os serviços IP para acesso dedicado à Internet global, com os circuitos de acesso com a mesma capacidade de tráfego nos dois sentidos.

1.1.4. A CONTRATADA deverá fornecer toda a infraestrutura necessária para disponibilizar os serviços de Rede MPLS de forma dedicada e exclusiva, ou seja, não compartilhada. Os circuitos de acesso a esta Rede devem possuir a mesma capacidade de tráfego nos dois sentidos.

1.2. Serviço de Suporte Técnico

1.2.1. O serviço de suporte técnico consiste em manutenção preventiva e manutenção corretiva dos itens que compõem a solução contratada;

1.2.2. O período de suporte técnico, manutenção e garantia tem a vigência do contrato estabelecido para fornecimento do objeto do TR;

1.2.3. As atividades serão precedidas da abertura de um chamado técnico;

1.2.4. A CONTRATANTE poderá efetuar um número ilimitado de chamados durante a vigência do contrato;

1.2.5. A CONTRATADA deverá acordar com a Funasa as interrupções programadas com antecedência mínima de 7 (dias) dias úteis e deverão ser realizadas, de preferência, aos finais de semana ou feriados.

1.2.6. Nos casos em que a realização dos serviços de suporte técnico necessitarem de parada da solução, a CONTRATANTE deverá ser imediatamente notificada para que se proceda a autorização do suporte técnico, ou para que seja agendada nova data, a ser definida pela CONTRATANTE, para a realização do referido serviço de suporte;

1.2.7. O serviço de suporte técnico deverá ser realizado em regime de 24 (vinte e quatro) horas por 7 (sete) dias por semana, todos os dias do ano, no idioma português, devendo a empresa possuir uma central de atendimento sem custos para a CONTRATANTE e atender aos chamados da equipe técnica nos prazos estabelecidos no TR;

1.2.8. Durante o período de vigência do contrato e do suporte técnico e garantia, quando for o caso, todos os firmwares e softwares deverão ser atualizados a cada nova versão ou correção, sem nenhum custo adicional para a CONTRATANTE;

1.2.9. O serviço de suporte técnico poderá ser atendido através de contato telefônico, por e-mail ou presencial, sendo este critério decidido pela equipe técnica da CONTRATANTE;

1.2.10. Todos os prazos para atendimento dos chamados serão iniciados a partir da abertura do mesmo independentemente deste ter sido feito via telefone, e-mail ou website da CONTRATADA;

1.2.11. A CONTRATADA deverá disponibilizar um sistema de abertura de chamados para que a CONTRATANTE possa receber um identificador único para cada solicitação de atendimento e que tenha recursos (e-mail, página web, central telefônica ou etc.) que

possam manter a equipe técnica da CONTRATANTE informada sobre o andamento de cada chamado, esteja ele aberto, em andamento ou fechado;

1.2.12. Os serviços serão classificados pela Equipe Técnica da CONTRATANTE, quando da abertura dos chamados técnicos, segundo sua prioridade e obedecendo aos Níveis de Serviço;

1.2.13. A Funasa considerará efetivamente realizado o serviço quando houver confirmação por sua área técnica da conclusão satisfatória do atendimento;

1.2.14. Todos os chamados técnicos somente poderão ser encerrados com a anuência da CONTRATADA e da CONTRATANTE;

1.2.15. Qualquer chamado fechado, sem anuência da CONTRATANTE ou sem que o problema tenha sido de fato resolvido, será reaberto e os prazos serão contados a partir da abertura original do chamado;

1.2.16. A CONTRATADA manterá cadastro das pessoas indicadas pela CONTRATANTE que poderão efetuar abertura e fechamento de chamados;

1.2.17. A CONTRATADA deverá garantir, quando da execução dos serviços, o repasse dos conhecimentos teóricos e práticos que fundamentarem a solução dos problemas à equipe técnica da CONTRATANTE;

1.2.18. A CONTRATADA deverá dispor de equipe técnica capacitada para executar os serviços contratados de forma on-site, quando necessário;

1.2.19. Deverão ser emitidos, relatórios mensais referentes ao histórico dos incidentes, e atendimentos de suporte e manutenção independentemente de seu estado (abertos, fechado e em andamento).

1.3. Serviço de Gerenciamento da Rede

1.3.1. A CONTRATADA deverá prover um serviço de Gerenciamento da Rede que contemple as áreas funcionais de gestão de falhas, gestão de desempenho, gestão de configuração, gestão de segurança e de nível de serviço. O serviço deverá atender, no mínimo, às seguintes funcionalidades:

1.3.1.1. Abertura, acompanhamento e encerramento de chamados técnicos;

1.3.1.2. Geração e emissão de relatórios gerenciais que permitam o acompanhamento da qualidade dos serviços, dos níveis de serviço contratados e a validação das faturas.

1.3.2. O Serviço de Gerenciamento da Rede Contratada deverá abranger todos os equipamentos e enlaces, independentemente de suas tecnologias, necessários a prestação dos serviços contratados;

1.3.3. A CONTRATADA deverá disponibilizar uma Central de Atendimento Especializado em Rede e Segurança, com número telefônico único, não tarifado (0800), para registro dos chamados, operando 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, todos os dias do ano. Poderá ser disponibilizada pela CONTRATADA uma Central de Atendimento Especializada e exclusiva para a Gestão da Segurança.

1.3.4. A Funasa deverá ter acesso via rede mundial de computadores (internet) para acompanhamento dos chamados técnicos abertos, bem como dos relatórios de estatísticas e históricos dos chamados.

1.3.5. Os chamados abertos na Central de Atendimento Especializado poderão ser referentes a todas as atividades de responsabilidade da CONTRATADA considerando os serviços contratados, englobando, mas não se limitando a: instalação, configuração, recuperação, alteração e remoção de equipamentos, enlaces, roteamento, endereçamento IP entre outros.

1.3.6. Os chamados registrados pela gerência proativa ou pela Funasa deverão ser registrados no sistema de atendimento e disponibilizado de forma clara, compreensível e facilmente legível, devendo compreender as seguintes informações mínimas:
  1.3.6.1. Número do chamado registrado e nível de severidade, inclusive aqueles com reabertura;
  1.3.6.2. Data e hora de abertura do chamado técnico (horário de Brasília/DF);
  1.3.6.3. Identificação do link que apresenta a falha/interrupção;
  1.3.6.4. Identificação do funcionário da CONTRATANTE, responsável pela abertura do chamado;
  1.3.6.5. Identificação do técnico da CONTRATADA responsável pela execução do serviço de normalização do circuito ou equipamento;
  1.3.6.6. Descrição do problema apresentado;
  1.3.6.7. Descrição da solução;
  1.3.6.8. Status da solicitação (chamado em aberto, pendentes ou fechados);
  1.3.6.9. Data e hora da execução dos serviços necessários;
  1.3.6.10. Data e hora do encerramento do chamado.

1.3.7. A CONTRATADA emitirá relatórios sempre que solicitados pela CONTRATANTE, em papel e em arquivo eletrônico, preferencialmente nos formatos .DOC, .DOCX ou .PDF, com informações analíticas e sintéticas dos chamados abertos e fechados no período, total de chamados no mês e o total acumulado até a apresentação do relatório, com no mínimo as informações do item 1.3.6;

1.3.8. A CONTRATADA deverá armazenar todos os dados coletados nos elementos gerenciados e as informações geradas para confecção dos relatórios durante a vigência do contrato, devendo ao final do contrato disponibilizá-los para a Funasa em meio eletrônico, a ser acordado entre as partes posteriormente.

1.3.9. A CONTRATADA deverá disponibilizar, a qualquer tempo, sua base de dados de gerenciamento e de atendimentos prestados à Funasa, conjuntamente com o modelo de dados, para que Fundação possa gerar relatórios com a finalidade de acompanhamento, averiguação e auditoria.

1.3.10. A CONTRATADA deverá responsabilizar-se pela integridade e sigilo dos dados coletados armazenados em sua infraestrutura, relativos à gerência, aos chamados registrados e seus solicitantes.

1.3.11. A CONTRATADA deverá demonstrar ao quadro técnico da Funasa que os circuitos atendem as características especificadas no Termo de Referência, no ato da entrega do circuito ou a qualquer momento que a Fundação vier a solicitar.

1.3.12. A CONTRATADA deverá prestar um serviço de gerenciamento proativo que a capacite a detectar as falhas (fim a fim), incluindo todos os equipamentos que compõem a infraestrutura dos serviços contratados, gerar alarmes automáticos e dar início ao processo de recuperação dos serviços de forma autônoma em no máximo 10 (dez) minutos, sem a necessidade de reclamação técnica por parte da Funasa.

1.3.13. A ferramenta de gerenciamento a ser disponibilizada para acesso pela Funasa deverá gerar alarmes automáticos, relatórios e consultas para cada um dos links, informando sobre:
  1.3.13.1. Quedas de desempenho;
  1.3.13.2. Incremento de taxa de erros;
  1.3.13.3. Perda de pacotes;
  1.3.13.4. Aumento de latência.
  1.3.13.5. Relatório gerencial;

1.3.13.6. Relatório operacional;
1.3.13.7. Relatório consolidado;
1.3.13.8. Relatório detalhado;
1.3.13.9. Disponibilização de inventário: (informações sobre a localização física de ativos de rede como equipamentos CPE's, portas, placas e acessos);
1.3.13.10. Consulta de configuração corrente de equipamentos;
1.3.13.11. Consulta a inventário de equipamentos (modelos, fabricantes e interfaces);
1.3.13.12. Visão gráfica da rede com os respectivos alarmes;
1.3.13.13. Consulta de localidades (nomes, endereços);
1.3.13.14. Consulta de conexões (portas, sub-interfaces, velocidades, protocolos).

1.3.14. O sistema de gerenciamento proativo deverá funcionar 24 (vinte e quatro) horas por dia, todos os dias da semana.

1.3.15. A Funasa irá monitorar a rede contratada por meio de ferramenta, paralelamente ao sistema de gerenciamento fornecido pela CONTRATADA, devendo a CONTRATADA disponibilizar informações sobre os pontos de presença e de rede sempre que solicitado.

1.3.16. Deverá ser firmado um acordo operacional e de níveis de acesso aos equipamentos de rede, entre as partes contraentes, no qual deverão constar as informações necessárias ao processo operacional, como por exemplo: horário normal de funcionamento de cada link, desligamentos diários de equipamentos, contatos locais (nome, telefone, e-mail) e responsáveis por abertura de chamados, e outras informações que se fizerem necessárias à adequada operacionalização dos serviços.

1.3.17. A CONTRATADA deverá disponibilizar para a Funasa, um Relatório de Acompanhamento mensal, configurável e com filtros de fácil aplicação e remoção, de forma a permitir o acompanhamento da qualidade dos serviços prestados.

1.3.18. O relatório de acompanhamento mensal deve ser consolidado até o 5° (quinto) dia útil do mês subsequente para aferição dos serviços prestados no mês anterior, que deve ser entregue quando solicitado, e sempre em mídia digital;

1.3.19. Deverá ser firmado, entre as partes contraentes, um acordo de compartilhamento da operação e níveis de acesso à solução de segurança no qual deverão constar as informações necessárias ao processo operacional.

1.3.20. A gestão compartilhada inicia apenas após entrega dos equipamentos funcionando e com todas as regras iniciais implementadas e validadas pela CONTRATANTE.

~~1.3.21.~~ Entende-se por gestão compartilhada, a atuação da CONTRATANTE e da CONTRATADA em configuração do equipamento do ponto de vista operacional, ou seja, configurações de regras. ~~A atuação da CONTRATADA fica limitada a atuação de manutenção de hardware e evolução de versão e aplicação de patches corretivos ou evolutivos;~~

1.3.22. O acordo operacional poderá ser flexibilizado, desde que acordado por ambas as partes.

1.3.23. Faz parte deste acordo o compartilhamento da operação dos equipamentos de segurança, níveis de acesso à solução de segurança no qual deverão constar: os equipamentos que fazem parte deste acordo, quais ações serão de responsabilidade da equipe da Funasa e demais informações necessárias ao processo operacional.

1.3.24. As falhas ou interrupções em decorrência da operação por parte da Funasa não acarretarão penalidades à CONTRATADA.

1.3.25. O relatório de acompanhamento mensal deve conter, no mínimo:

1.3.25.1. Informação da gerência de desempenho com volume total de tráfego do período de referência;

1.3.25.2. Informações relativas à instalação, desinstalação, alteração de política de acesso ou tecnologia de acesso e remanejamento de links;

1.3.25.3. Informações sobre todos os chamados recebidos no período de referência: quantidade total de chamados recebidos, quantidade total de chamados por link, a quantidade total de chamados por estado de solicitação e quantidade total de indisponibilidade por link;

1.3.25.4. Resumo dos chamados que geraram indisponibilidade no período de referência.

1.4. Serviço de Gerenciamento e Monitoramento de Segurança da Rede

1.4.1. A CONTRATADA deverá prover um serviço de Gerenciamento de Segurança da Rede que contemple as áreas funcionais de gestão de falhas, gestão de desempenho, gestão incidentes de segurança;

1.4.2. O Serviço de Gerenciamento proativo de Segurança da Rede deverá abranger todos os equipamentos de segurança contratados independentemente de suas tecnologias, necessários a prestação dos serviços, devendo funcionar 24 (vinte e quatro) horas por dia, todos os dias da semana;

1.4.3. Cabe à CONTRATADA acionar o suporte técnico de rede para correção de falhas na infraestrutura que esteja comprometendo o serviço de segurança;

1.4.4. Cabe à CONTRATADA acionar quando necessário o fabricante do equipamento que compõem a solução de segurança;

1.4.5. Cabe à CONTRATADA monitorar, diagnosticar e corrigir falhas que envolvam toda a infraestrutura e equipamentos de rede e de segurança entregues por ela, devendo, portanto, haver uma interação entre as equipes de suporte de rede e suporte de segurança, garantido uma completa integração entre todos os equipamentos e uma perfeita prestação do serviço contratado.

1.4.6. Cabe à CONTRATADA iniciar a recuperação dos serviços de forma autônoma em no máximo 15 (quinze) minutos, sem a necessidade de abertura de requisição técnica por parte da Funasa. Para efeito de contabilização do tempo de atendimento destes incidentes será considerado o tempo de identificação por parte da ferramenta de monitoramento da Contratada ou da abertura de chamado pela Funasa, o que ocorrer primeiro.

1.4.7. A CONTRATADA deverá disponibilizar uma Central de Atendimento Especializado em Segurança de Rede, com número telefônico único, não tarifado (0800), para registro dos chamados, operando 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, todos os dias do ano. Poderá ser disponibilizada pela CONTRATADA uma Central de Atendimento Especializada compartilhada com a gestão da Rede.

1.4.8. A Funasa deverá ter acesso via rede mundial de computadores (internet) para acompanhamento dos chamados técnicos abertos, bem como dos relatórios de estatísticas e históricos dos chamados.

1.4.9. Nos casos de incidentes ou problemas no ambiente gerenciado de segurança da Rede Funasa, as intervenções preventivas ou reativas serão identificadas, registradas e classificadas pela CONTRATADA ou, excepcionalmente, pelo CONTRATANTE, conforme sua severidade;

1.4.10. Para os chamados de suporte categorizado como Severidade Crítica ou Alta, o atendimento não pode ser interrompido até o completo restabelecimento de todas as

funções do item gerenciado de segurança que esteja paralisado ou indisponível, mesmo que para isso tenham que se estender por períodos noturnos e dias não úteis (sábados, domingos e feriados), de acordo com a disponibilidade da Funasa;

1.4.11. Cada requisição ou incidente identificado pela gerência proativa ou pela Funasa deverá ser registrado no sistema de atendimento e disponibilizado de forma clara, compreensível e facilmente legível, devendo compreender as seguintes informações mínimas:

1.4.11.1. Número do chamado registrado e nível de severidade ou prioridade, inclusive aqueles com reabertura;

1.4.11.2. Data e hora de abertura do chamado técnico (horário de Brasília/DF);

1.4.11.3. Identificação do ponto de presença que apresenta a falha/interrupção;

1.4.11.4. Identificação do funcionário do CONTRATANTE, responsável pela abertura do chamado;

1.4.11.5. Identificação do técnico da CONTRATADA responsável pela execução do serviço de normalização do circuito ou equipamento;

1.4.11.6. Descrição do problema apresentado;

1.4.11.7. Descrição da solução;

1.4.11.8. Status da solicitação (chamado em aberto, pendentes ou fechados);

1.4.11.9. Data e hora da execução dos serviços necessários;

1.4.11.10. Data e hora do encerramento do chamado.

1.4.12. A CONTRATADA emitirá relatórios sempre que solicitados pela CONTRATANTE, com informações analíticas e sintéticas dos chamados abertos e fechados no período, com no mínimo as informações coletadas no subitem 1.4.11;

1.4.13. A CONTRATADA deverá armazenar todos os dados coletados nos elementos gerenciados de segurança geradas para confecção dos relatórios durante a vigência do contrato, devendo ao final do contrato disponibilizá-los para a Funasa em meio eletrônico, a ser acordado entre as partes posteriormente;

1.4.14. A CONTRATADA deverá disponibilizar, a qualquer tempo, sua base de dados de gerenciamento e de atendimentos prestados para a Funasa, conjuntamente com o modelo de dados, para que a Fundação possa gerar relatórios com a finalidade de acompanhamento, averiguação e auditoria;

1.4.15. A CONTRATADA deverá responsabilizar-se pela integridade e sigilo dos dados coletados armazenados em sua infraestrutura, relativos à gerência, aos chamados registrados e seus solicitantes, atendendo ao que estabelece a LGPD;

1.4.16. A CONTRATADA deverá disponibilizar para a Funasa, Relatórios gerenciais mensais que permitam o acompanhamento da qualidade, disponibilidade e nível dos serviços prestados, com vistas a validação das faturas, devendo conter, no mínimo:

1.4.16.1. Informações relativas à reparos, manutenções e trocas de equipamentos;

1.4.16.2. Informações sobre todos os chamados relativos a incidentes e requisições recebidas no período de referência: quantidade total de chamados registrados, quantidade total de chamados por pontos de presença, a quantidade total de chamados por situação (status) das solicitações e quantidade total de indisponibilidade por pontos de presença;

1.4.16.3. Abertura, acompanhamento e encerramento de chamados técnicos;

1.4.16.4. Total de chamados no mês e o total acumulado até a apresentação do relatório.

1.4.17. O relatório de acompanhamento mensal deve ser consolidado até o 5° (quinto) dia útil do mês subsequente para aferição dos serviços prestados no mês anterior, sempre em mídia digital;
1.4.18. Deverá apresentar, quando solicitado, um relatório que demonstre o nível de segurança de seus equipamentos e as recomendações dos fabricantes quanto a melhoria em sistemas operacionais e configurações que compõem a solução contratada, visando detectar possíveis falhas no serviço e na segurança da rede.
1.4.19. Além destes indicadores de nível de serviço apresentados, outros podem ser definidos a qualquer tempo de comum acordo entre a Funasa e a CONTRATADA, permitindo desta forma, a melhoria continua a partir do próprio aprendizado que os atores forem adquirindo com a execução dos serviços.
1.4.20. A CONTRATADA deverá fazer constar no relatório de acompanhamento mensal a informação dos links que ficaram sem conectividade por mais de 5 (cinco) dias corridos.
1.4.21. A CONTRATADA deverá notificar sobre indisponibilidade de um link quando esse ficar indisponível por mais de 2(duas) horas;
1.4.22. Só poderão ser cobrados os serviços efetivamente ativados e em operação, ou seja, os serviços que foram aceitos pela Funasa.

1.5. Serviço de Proteção Contra Ataques "DDoS"

1.5.1. A CONTRATADA deverá disponibilizar em seu backbone proteção contra os ataques de negação de serviços DoS e DDoS, evitando assim a saturação da banda da Internet e a indisponibilidade dos serviços da Funasa;
1.5.2. O Serviço deverá ter pró-atividade na prevenção e tratamento de incidentes e ataques;
1.5.3. Deverá monitorar a disponibilidade e desempenho do link de dados do tipo C1 - Internet Corporativo contemplado no TR em regime 24x7, utilizando profissionais de forma dedicada;
1.5.4. Deverá tomar todas as providencias necessárias para recompor a disponibilidade do link em caso de incidentes de ataques de DDoS, recuperando seu pleno funcionamento;
1.5.5. Deverá possuir a capacidade de criar e analisar a reputação de endereços IP, possuindo base de informações próprias, gerada durante a filtragem de ataques, e interligada com os principais centros mundiais de avaliação de reputação de endereços IP;
1.5.6. Deverá suportar a mitigação automática de ataques, utilizando múltiplas técnicas como White Lists, Black Lists, limitação de taxa, técnicas desafio-resposta, descarte de pacotes mal-formados, técnicas de mitigação de ataques aos protocolos HTTP e DNS, bloqueio por localização geográfica de endereços IP, dentre outras;
1.5.7. Deverá implementar mecanismos capazes de detectar e mitigar todos e quaisquer ataques que façam o uso não autorizado de recursos de rede, incluindo, mas não se restringindo às seguintes categorias de ataques:
1.5.7.1. Ataques de inundação (Bandwidth Flood), incluindo Flood de UDP e ICMP;
1.5.7.2. Ataques a pilha TCP, incluindo mal uso das Flags TCP, ataques de RST e FIN, SYN Flood e TCP Idle Resets;
1.5.7.3. Ataques que utilizam fragmentação de pacotes, incluindo pacotes IP, TCP e UDP;
1.5.7.4. Ataques de Botnets, Worms e ataques que utilizam falsificação de endereços IP de origem (IP Spoofing);
1.5.7.5. Ataques a camada de aplicação, incluindo protocolos HTTP e DNS;

1.5.8. A solução deve manter uma lista dinâmica de endereços IP bloqueados, retirando dessa lista os endereços que não enviarem mais requisições maliciosas após um período considerado seguro pela CONTRATADA;

1.5.9. A CONTRATADA deve possuir centro de limpeza nacional e internacional com capacidade de mitigação; a

1.5.10. A CONTRATADA deve mitigar ataques enquanto o ataque não tiver sido cessado;

1.5.11. Caso o volume de tráfego do ataque ultrapasse as capacidades de mitigação especificadas ou sature as conexões do AS, devem ser tomadas contramedidas tais como aquelas que permitam o bloqueio seletivo por blocos de IP de origem no AS pelo qual o ataque esteja ocorrendo, utilizando técnicas como Remote Triggered Black Hole;

1.5.12. As soluções de detecção e mitigação devem possuir serviço de atualização de assinaturas de ataques;

1.5.13. A CONTRATADA deve disponibilizar um Centro de Operação de Segurança (SOC — Security Operations Center) no Brasil, com equipe especializada em monitoramento, detecção e mitigação de ataques, com opção de atendimento através de telefone 0800, correio eletrônico, em idioma português brasileiro, durante as 24 (vinte e quatro) horas do dia, nos 7 (sete) dias da semana, no período de vigência contratual.

1.5.14. A mitigação de ataques deve ser baseada em arquitetura na qual haja o desvio de trafego suspeito comandado pelo equipamento de monitoramento, por meio de alterações do plano de roteamento;

1.5.15. Em eventos de ataques DoS e DDoS, todo tráfego limpo deve ser reinjetado na infraestrutura da CONTRATANTE através de tuneis GRE (Generic Routing Encapsulation), configurado entre a plataforma de DoS e DDoS da CONTRATADA e o CPE do CONTRATANTE;

1.5.16. Para a mitigação dos ataques não será permitido o encaminhamento do tráfego para limpeza fora do território brasileiro;

1.5.17. As funcionalidades de monitoramento, detecção e mitigação de ataques devem ser mantidas em operação ininterrupta durante as 24(vinte e quatro) horas do dia, nos 7 (sete) dias da semana, no período de vigência contratual;

1.5.18. Em nenhum caso será aceito bloqueio de ataques de DoS e DDoS por ACLs em roteadores de bordas da CONTRATADA;

1.5.19. A CONTRATADA deve iniciar a mitigação de ataques de DDoS em no máximo 15 minutos;

1.5.20. A ferramenta de gerenciamento a ser disponibilizada para acesso pela Funasa deverá atender aos seguintes requisitos:

1.5.20.1. Deverá atribuir a cada alerta um número de identificação que facilite sua consulta;

1.5.20.2. Deverá registrar a data de início e fim do acompanhamento do alerta;

1.5.20.3. Disponibilizar relatórios e consultas sobre o volume de ataques sumarizados por hora, dia, semana e mês;

1.5.20.4. Relatório por tipos de ataques;

1.5.21. O Portal de monitoração da CONTRATADA devera possuir uma interface única para acesso as suas funcionalidades, independentemente dos equipamentos ou tecnologias empregadas para a prestação dos serviços;

1.5.22. O Portal de Gerência deverá permitir o acesso simultâneo a, pelo menos, dois administradores de rede da CONTRATANTE;

2. Características dos Equipamentos

2.1. Tipo-1 - CPE conectividade para os circuitos C1, C2 e C4

2.1.1. O roteador deverá ser dimensionado para atender o serviço na capacidade máxima especificada;
2.1.2. O roteador CPE deverá ser fornecido com todos os componentes, módulos e acessórios necessários ao seu perfeito funcionamento;
2.1.3. A configuração lógica do roteador CPE será definida pela CONTRATADA com a aprovação da Funasa.
2.1.4. Todos os roteadores suportarão, além dos protocolos básicos para operação em uma rede IP com compressão de dados e o protocolo de roteamento OSPF, com opção de security telnet e IPsecurity (IPSec);
2.1.5. Os roteadores terão facilidades de configuração e checagem por meio de porta serial e da console de monitoramento.
2.1.6. O roteador CPE deve ser modular;
2.1.7. Deverá ser instalado com no mínimo 2 interfaces 10GbE padrão SFP+, expansível a no mínimo 4 interfaces, quando necessário;
2.1.8. Deverá ser instalado com no mínimo 04 (quatro) interface LAN 100/1000BASE-T com slots RJ-45, expansível a no mínimo 8 interfaces;
2.1.9. Deve suportar fontes AC redundantes;
2.1.10. Deve possuir suporte a 4094 VLAN Tags 802.1q;
2.1.11. Deve possuir suporte a agregação de links 802.3ad e LACP;
2.1.12. Deve possuir suporte a Policy based routing ou policy based forwarding;
2.1.13. Deve possuir suporte a roteamento multicast (PIM-SM e PIM-DM);
2.1.14. Deve possuir suporte a DHCP Relay;
2.1.15. Deve possuir suporte a DHCP Server;
2.1.16. Deve suportar sFlow;
2.1.17. Deve possuir suporte a Jumbo Frames;
2.1.18. Deve suportar sub-interfaces ethernet lógicas;
2.1.19. Deve implementar o protocolo ECMP;
2.1.20. Deve permitir monitorar via SNMP;
2.1.21. Enviar log para sistemas de monitoração externos, simultaneamente;
2.1.22. Possuir a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;
2.1.23. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
2.1.24. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);
2.1.25. Suportar OSPF graceful restart;
2.1.26. Deve suportar o padrão de indústria 'syslog' protocol para armazenamento usando o formato Common Event Format (CEF);
2.1.27. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem;
2.1.28. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de destino;
2.1.29. Suportar a criação de políticas de QoS e Traffic Shaping por porta;
2.1.30. O QoS deve possibilitar a definição de tráfego com banda garantida;
2.1.31. O QoS deve possibilitar a definição de tráfego com banda máxima;
2.1.32. O QoS deve possibilitar a definição de fila de prioridade;
2.1.33. Suportar marcação de pacotes Diffserv, inclusive por aplicação;
2.1.34. Suportar modificação de valores DSCP para o Diffserv;
2.1.35. Suportar priorização de tráfego usando informação de Type of Service;

2.1.36. Deve suportar QOS (traffic-shapping), em interface agregadas ou redundantes;
2.1.37. Suportar IPSec VPN;
2.1.38. A VPN IPSEc deve suportar Autenticação MD5 e SHA-1;
2.1.39. A VPN IPSEc deve suportar Diffie-Hellman Groups;
2.1.40. A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1);
2.1.41. A VPN IPSEc deve suportar AES (Advanced Encryp on Standard);
2.1.42. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall, HPE/Aruba.

2.2. TIPO-2 - CPE equipamentos de conectividade para os circuitos C3.1 e C3.2

2.2.1. Os roteadores deverão ser dimensionados para atender o serviço na capacidade máxima especificada, sem a necessidade de troca de equipamento e devem possuir as seguintes características:
2.2.2. Throughput mínimo suficiente para suportar todo o tráfego de dados sem degradação;
2.2.3. Os equipamentos de conectividade de rede devem possuir suporte a Vlans;
2.2.4. Devem possuir suporte a agregação de links 802.3ad e LACP;
2.2.5. Devem possuir suporte a Policy based routing ou policy based forwarding;
2.2.6. Devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);
2.2.7. Devem suportar BGP, OSPF, RIP e roteamento estático;
2.2.8. Devem possuir suporte a DHCP Relay;
2.2.9. Devem possuir suporte a DHCP Server;
2.2.10. Devem possuir suporte a Jumbo Frames;
2.2.11. Devem suportar sub-interfaces ethernet logicas;
2.2.12. Devem suportar NAT dinâmico (Many-to-Many);
2.2.13. Devem suportar NAT estático (1-to-1);
2.2.14. Devem suportar NAT estático bidirecional 1-to-1;
2.2.15. Devem suportar Tradução de porta (PAT);
2.2.16. Devem suportar NAT de Origem;
2.2.17. Devem suportar NAT de Destino;
2.2.18. Devem suportar NAT de Origem e NAT de Destino simultaneamente;
2.2.19. Devem implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
2.2.20. Devem suportar NAT64 e NAT46;
2.2.21. Devem suportar roteamento estático e dinâmico (RIP, BGP e OSPF);
2.2.22. Devem permitir monitorar via SNMP, no mínimo, o uso de CPU, memória e interfaces;
2.2.23. Devem enviar log para sistemas de monitoração externo, inclusive via protocolo SSL;
2.2.24. Os equipamentos deverão possuir, no mínimo, 04 (quatro) interface LAN 100/1000BASE-T com slots RJ-45, com capacidade de expansão;
2.2.25. Para os circuitos C3 e C5, as funcionalidades de CPE e NGFW, que compõem a solução, podem funcionar em equipamento único obedecendo a todos os requisitos desta especificação, com suporte de gerenciamento centralizado;
2.2.26. Para os circuitos C3 e C5, as funcionalidades de CPE podem ser fornecidas no equipamento NGFW ofertado ou em equipamento à parte, neste caso, devem ser entregues na mesma quantidade do equipamento NGFW.

3. Funcionalidades

3.1.1. Funcionalidades de Controle de Políticas

3.1.1.1. Deve suportar controles por zonas de segurança;
3.1.1.2. Deve suportar controles de políticas por porta e protocolo;
3.1.1.3. Deve suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações;
3.1.1.4. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;
3.1.1.5. Controle de políticas por código de País (Por exemplo: BR, US, UK, RU);
3.1.1.6. Controle, inspeção e descriptografia de SSL por políticas para tráfego de saída (Outbound);
3.1.1.7. Deve descriptografar tráfego outbound em conexões negociadas com TLS 1.2 e TLS 1.3;
3.1.1.8. Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada;
3.1.1.9. Suporte a objetos e regras IPV6;
3.1.1.10. Suporte a objetos e regras multicast;
3.1.1.11. Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.

3.1.2. Controle de Aplicações

3.1.2.1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;
3.1.2.2. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;
3.1.2.3. Reconhecer pelo menos 1700 aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;
3.1.2.4. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive,skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting,webex, evernote, google-docs, instagram, aplicativos de relacionamento e jogos;
3.1.2.5. Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;
3.1.2.6. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;
3.1.2.7. Para tráfego criptografado SSL, deve descriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;

3.1.2.8. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo. A decodificação de protocolo também deve identificar funcionalidades especificas dentro de uma aplicação;

3.1.2.9. Identificar o uso de táticas evasivas via comunicações criptografadas;

3.1.2.10. Atualizar a base de assinaturas de aplicações automaticamente;

3.1.2.11. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;

3.1.2.12. Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;

3.1.2.13. Deve suportar vários métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;

3.1.2.14. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;

3.1.2.15. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;

3.1.2.16. Deve alertar o usuário quando uma aplicação for bloqueada;

3.1.2.17. Deve possibilitar a diferenciação de tráfegos Peer-to-Peer (Bittorrent, emule, etc.) possuindo granularidade de controle/políticas para os mesmos;

3.1.2.18. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc.) possuindo granularidade de controle/políticas para os mesmos;

3.1.2.19. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts e bloquear a chamada de vídeo;

3.1.2.20. Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc.) possuindo granularidade de controle/políticas para os mesmos;

3.1.2.21. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc.);

3.1.2.22. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: nível de risco da aplicação e categoria da aplicação;

3.1.2.23. Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação.

3.1.3. Prevenção de Ameaças

3.1.3.1. Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware;

3.1.3.2. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);

3.1.3.3. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;

3.1.3.4. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear e quarentenar IP do atacante por um intervalo de tempo;
3.1.3.5. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;
3.1.3.6. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;
3.1.3.7. Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura;
3.1.3.8. Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
3.1.3.9. Deve permitir o bloqueio de vulnerabilidades;
3.1.3.10. Deve permitir o bloqueio de exploits conhecidos;
3.1.3.11. Deve incluir proteção contra-ataques de negação de serviços;
3.1.3.12. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc.;
3.1.3.13. Detectar e bloquear a origem de port scans;
3.1.3.14. Bloquear ataques efetuados por worms conhecidos;
3.1.3.15. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;
3.1.3.16. Possuir assinaturas para bloqueio de ataques de buffer overflow;
3.1.3.17. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;
3.1.3.18. Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações;
3.1.3.19. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
3.1.3.20. Identificar e bloquear comunicação com botnets;
3.1.3.21. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
3.1.3.22. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;
3.1.3.23. Os eventos devem identificar o país de onde partiu a ameaça;
3.1.3.24. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;
3.1.3.25. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;
3.1.3.26. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando usuários, grupos de usuários, origem, destino, zonas de segurança, etc., ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.
3.1.3.27. Deve ser capaz de mitigar ameaças avançadas persistentes (APT), através de análises dinâmicas para identificação de malwares desconhecidos;

3.1.3.28. Dentre as análises efetuadas, a solução deve suportar antivírus, query na nuvem, emulação de código, sandboxing e verificação de call-back;

3.1.3.29. A solução deve analisar o comportamento de arquivos suspeitos em um ambiente controlado;

3.1.4. Filtro de URLs

3.1.4.1. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

3.1.4.2. Deve ser possível a criação de políticas por grupos de usuários, IPs, redes ou zonas de segurança;

3.1.4.3. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local;

3.1.4.4. A identificação pela base do Active Directory deve permitir SSO, de forma que os usuários não precisem logar novamente na rede para navegar pelo firewall;

3.1.4.5. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;

3.1.4.6. Possuir categorias de URLs previamente definidas pelo fabricante e atualizáveis a qualquer tempo;

3.1.4.7. Possuir pelo menos 70 categorias de URLs;

3.1.4.8. Deve possuir a função de exclusão de URLs do bloqueio;

3.1.4.9. Permitir a customização de página de bloqueio;

3.1.4.10. Permitir a restrição de acesso a canais específicos do Youtube, possibilitando configurar uma lista de canais liberado ou uma lista de canais bloqueados;

3.1.4.11. Deve bloquear o acesso a conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, independentemente de a opção Safe Search estar habilitada no navegador do usuário.

3.1.5. Identificação de Usuários

3.1.5.1. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-directory e base de dados local;

3.1.5.2. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

3.1.5.3. Deve possuir integração e suporte a Microsoft Active Directory para o sistema operacional Windows Server 2012 R2;

3.1.5.4. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários;

3.1.5.5. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

3.1.5.6. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;

3.1.5.7. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);
3.1.5.8. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
3.1.5.9. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;
3.1.5.10. A solução deve suportar autenticação de usuários com credenciais de mídias sociais de terceiros como Facebook, Twitter, LinkedIn e Google+;
3.1.5.11. A solução deve permitir que usuários que não possuam uma conta local ou em mídias sociais se autentiquem através de umrápido cadastro, que garanta o mínimo de rastreabilidade, através da validação de endereços de e-mail ou número de telefone;
3.1.5.12. A solução deve permitir o login automático de usuários visitantes depois de se registrarem com sucesso;
3.1.5.13. Deve suportar Security Assertion Markup Language (SAML), agindo como um Provedor de Identidade (Indentity Provider - IDP) estabelecendo um relacionamento de confiança para autenticação segura de usuários tentando acessar um Provedor de Serviços (ServiceProvider -SP);

3.1.6. Filtro de Dados

3.1.6.1. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc.) identificados sobre aplicações (HTTP, FTP, SMTP, etc.);
3.1.6.2. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
3.1.6.3. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
3.1.6.4. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular.
3.1.6.5. GEOLOCALIZAÇÃO
3.1.6.6. Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados;
3.1.6.7. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;
3.1.6.8. VPN
3.1.6.9. Suportar VPN IPSec Site-to-Site;
3.1.6.10. A VPN IPSEC deve suportar criptografia 3DES, AES128, AES192 e AES256 (Advanced Encryption Standard);
3.1.6.11. A VPN IPSEc deve suportar Autenticação MD5, SHA1, SHA256, SHA384 e SHA512;
3.1.6.12. A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14, Group 15 até 21 e Group 27 até 32;
3.1.6.13. A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);
3.1.6.14. A VPN IPSEc deve suportar Autenticação via certificado IKE PKI;

3.1.6.15. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;

Anexo X - Anexo X - Arquitetura da Rede Funasa.pdf

Anexo X – ARQUITETURA DA REDE FUNASA

SUMÁRIO

1. Estrutura e objetivos da Rede Funasa

1.1. A arquitetura da Rede Funasa será constituída de conexões VPN MPLS e Internet, que permitirão a comunicação e interligação de longa distância entre os sites remotos e o ponto central de processamento de dados, em Brasília (DF), onde estão hospedados os serviços disponibilizados pela Fundação.

1.2. A Rede Funasa consistirá em infraestrutura de telecomunicações a ser utilizada pela autarquia, incluindo as Superintendências Estaduais - SUEST e unidades descentralizadas. Essas unidades estarão interconectadas à Rede Funasa através da Internet ou backbone MPLS. Esta rede deverá prover infraestrutura física e lógica para que os serviços de correio eletrônico, acesso à Internet, transferência de arquivos, autenticação de usuários, integração de sistemas legados, gerência e segurança da informação e demais sistemas.

1.3. Esta rede permitirá ainda a adoção de mecanismos que melhorem a conectividade e a velocidade das conexões, agreguem novos serviços colaborativos, elevem a segurança das operações realizadas, com especial atenção aos aspectos de disponibilidade, integridade e confidencialidade das informações trafegadas.

2. Premissas e restrições

2.1. As seguintes premissas e restrições foram adotadas no projeto:

- Será mantido todo o endereçamento IP privado utilizado nas LANs dos sites atuais, em conformidade com a RFC 1918;
- O Site Central da solução é localizado na sede da Funasa em Brasília.
- A Funasa irá indicar a quantidade e localização dos sites para as instalações-piloto;
- O QoS, quando necessário, será configurado de acordo com as políticas de QoS da Funasa;
- A CONTRATADA deverá garantir endereços IP fixos para todas as conexões de Internet, de modo a viabilizar o estabelecimento de VPN site to site, além dos endereços para os equipamentos fornecidos e gerenciados por ela; e
- Cabe à CGMTI a definição, gestão e todo o acompanhamento dos serviços contratados, sendo ela, portanto, o único interlocutor técnico junto à Contratada.

2.2. Consideram-se as convenções e nomenclaturas apresentadas na Especificação Técnica da Rede FUNASA, parte integrante do TR, que relaciona as categorias de links que integram a Rede Corporativa da Fundação com os fatores de desempenho, qualidade, prazo e suporte a serviços.

2.3. Categorias de links:

Item	Categoria	Descrição	Descrição
1	C1	Internet Corporativo – Nó Central – Dupla Abordagem com segurança	Link de dados em fibra óptica.
			Acesso de dupla abordagem com canal de comunicação de dados redundante que opere e se sustente por meios físicos distintos, desse modo, em caso de alguma indisponibilidade de um dos meios físicos, o serviço continuará operacional por caminho alternativo.
			Serviço de instalação em Brasília.
			Fornecimento, instalação e configuração de 1 Roteador CPE.

			Fornecimento, instalação e configuração de 2 equipamentos Cluster Firewall – NG, com funcionalidade UTM
			Fornecimento, instalação e configuração de 2 equipamentos Cluster SDWAN.
			Serviço de proteção contra ataques “DDoS”;
			Serviço de monitoramento; e
			Todos os implementos necessários à prestação do serviço.
2	C2	MPLS – Nó Central – Dupla Abordagem	Link de dados em fibra óptica.
			Destinado a receber todas as conexões MPLS dos circuitos C3.1 e C3.2.
			Acesso de dupla abordagem com canal de comunicação de dados redundante que opere e se sustente por meios físicos distintos, desse modo, em caso de alguma indisponibilidade de um dos meios físicos, o serviço continuará operacional por caminho alternativo.
			Serviço de instalação em Brasília.
			Fornecimento, instalação e configuração de 1 Roteador CPE, que deve ser interligado ao Firewall-NGFW e aos equipamentos SDWAN fornecidos no item 1.
			Serviço de monitoramento; e
			Todos os implementos necessários à prestação do serviço.
3	C3.1	MPLS - Link Corporativo - SUEST	Circuitos destinados à atender as Superintendências Estaduais
			Composto de link de dados terrestre em fibra óptica.
			Fornecimento, instalação e configuração de roteador CPE, 2 equipamentos Cluster Firewall – NG, com funcionalidade UTM
			Serviço de monitoramento e
			Todos os implementos necessários à prestação do serviço.
4	C3.2	MPLS - Link Corporativo - Unidades Descentralizadas	Circuitos destinados à atender as unidades descentralizadas.
			Composto de link de dados terrestre em fibra óptica.
			Fornecimento, instalação e configuração de roteador CPE, 2 equipamentos Cluster Firewall – NG, com funcionalidade UTM
			Serviço de monitoramento e
			Todos os implementos necessários à prestação do serviço.
5	C4	Lan-to-lan: SUEST GO	Composto de link de dados terrestre em fibra óptica.
			Serviço de instalação na Superintendência Estadual de Goiás.
			Acesso de dupla abordagem com canal de comunicação de dados redundante que opere e se sustente por meios físicos distintos, desse modo, em caso de alguma indisponibilidade de um dos meios físicos, o serviço continuará operacional por caminho alternativo;
			Fornecimento, instalação e configuração de Roteador CPE, 1 (um) equipamento TIPO-1.
			Serviço de monitoramento; e
			Todos os implementos necessários à prestação do serviço.

3. Equipamentos a serem entregues com a Rede

3.1. A Contratada deverá relacionar todos os equipamentos utilizados e especificados no Termo de Referência e seus Anexos, que atenderão aos requisitos e Níveis de Serviços estabelecidos.

4. Topologia da Rede Funasa

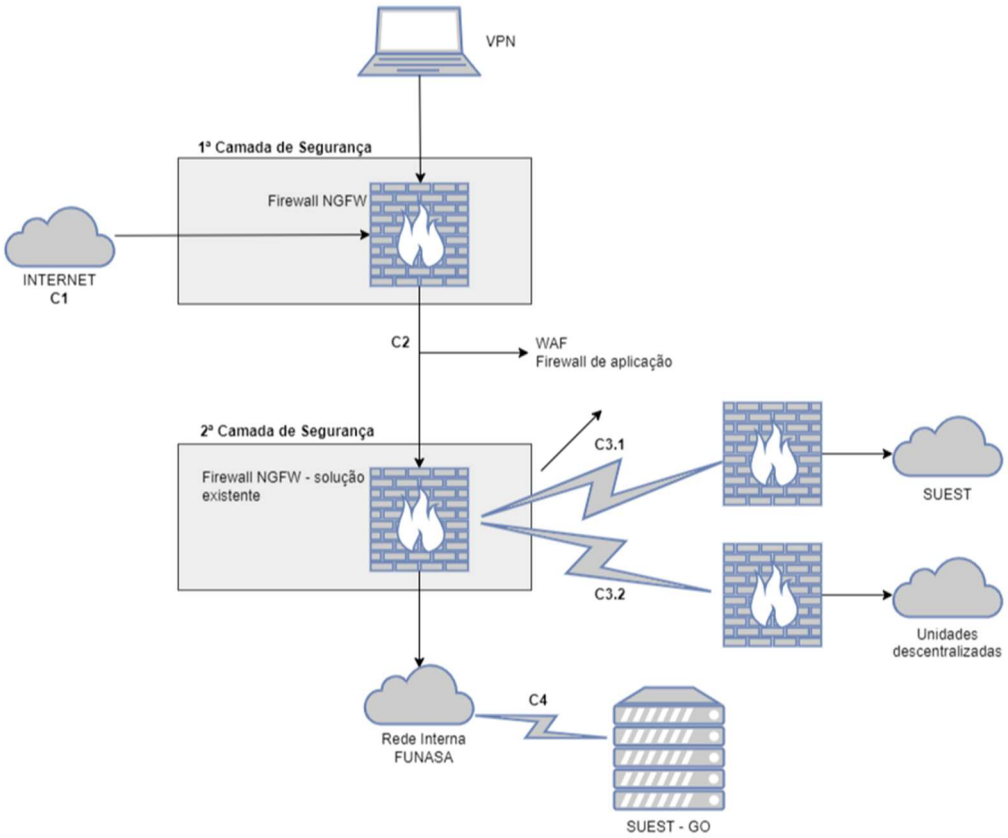

Figura 1 – Topologia Geral da Solução

4.1. Site Central

4.1.1. A Contratada fornecerá uma Rede MPLS para comunicação entre Site Central e Sites Remotos (SUEST e unidades descentralizadas);

4.1.2. O INTER-AS entre os Backbones MPLS, se aplicável, permitirá que os Sites Tipo C3.1 e C3.2 MPLS se comunique com o Site Central;

4.1.3. As aplicações e serviços da Funasa, que são suportados pela Rede Funasa, se concentram no Site Central Brasília, e serão providos por Links MPLS do Tipo C2 de 1Gbps, Link de Internet do Tipo C1 de 1 Gbps.

4.2. Superintendências Estaduais e Unidades Descentralizadas

4.2.1. Cada um destes sites será provido por 1 (um) link MPLS, Tipo C3.1, no caso das Superintendências Estaduais e Tipo C3.2, nas unidades descentralizadas, para atender em média 76 e um máximo de 142 estações, nas SUEST (considerado quantitativo prévio à extinção e recriação da autarquia);

4.3. Contingência L2L (Link de Replicação da solução de backup)

4.3.1. A replicação da solução de backup entre BSB e GO deverá ocorrer através do link L2L Tipo C4.

4.3.2. A gerência da rede da Funasa deve ter a capacidade de monitorar, em tempo real, a situação operacional do L2L por meio de acesso para esta finalidade ao CPE L2L local e também ao CPE L2L Remoto.

4.3.3. A Tecnologia SDWAN será utilizada no link de internet.

4.4. Configuração do SDWAN

4.4.1. A Tecnologia SDWAN será utilizada no link de internet.

4.4.2. Além do estabelecimento de túneis seguros, a tecnologia SDWAN possibilitará o roteamento dinâmico no Site central.

4.5. Roteamento e Contingência de acessos

4.5.1. Para que ocorra contingenciamento dos serviços MPLS e Internet, entre os equipamentos de borda do Site Central da Funasa e equipamentos da Contratada, será necessário habilitar roteamento dinâmico.

5. Endereçamento IP

5.1. Será utilizado para os CPEs MPLS a faixa de endereçamento IP privado, atualmente em uso pela Rede Funasa. Eventualmente, novas faixas de endereços poderão ser solicitados para a Funasa.

5.2. O endereçamento IP das redes LAN será o mesmo já em uso nos Sites da Funasa.

5.3. Para os CPEs dos link Tipo C1, o endereçamento WAN e endereçamento de gerência do equipamento deverão utilizar IPs válidos fornecidos pela Contratada.

6. QoS (Quality of Service)

6.1. Durante a execução do projeto de implementação, a Funasa informará os fluxos de tráfego pertencentes a cada classe de serviço para seleção, marcação e filtro dos pacotes para que tenham o tratamento esperado. Serão configurados os percentuais, definidos pela Funasa, das bandas de cada classe de serviço. A Contratada, quando solicitada, poderá auxiliar a Contratante na definição de padrões de QoS por Classe de serviço.

7. Gerência CPEs

7.1. Será disponibilizado para a Funasa usuários de leitura para acesso SSH ou Telnet aos CPEs da Contratada.

7.2. Os CPEs utilizarão autenticação de usuários de forma centralizada através servidor de autenticação da Contratada.

7.3. Deverá ser disponibilizado o envio de traps SNMP e configurado nos CPEs da Contratada Communities SNMP de leitura para utilização através do sistema de gerência de redes interno da Funasa.

7.4. Caso necessário, a Funasa também poderá efetuar a monitoração dos CPEs através de pacotes ICMP.

8. Segurança CPEs

8.1. Os acessos às portas Console, Auxiliar, Telnet e SSH serão todas autenticadas.
8.2. A senha de usuário local dos CPEs será criptografada ao ser visualizada na configuração do equipamento.
8.3. Deve ser utilizado ACL para restringir o acesso SSH ou Telnet aos CPEs da Contratada.
8.4. As sessões de Telnet e SSH terão, a critério da Funasa, seu tempo limitado, devendo ser desconectadas após inatividade.
8.5. Por padrão, os serviços DHCP e DNS serão desabilitados.
8.6. Os acessos SNMP e comunicação NTP serão limitados por ACL.
8.7. A critério da Funasa, poderão ser configuradas ACLs estáticas ou dinâmicas para bloqueio de tráfego indesejado nos CPEs remotos da Contratada.
8.8. Os CPEs terão sincronização de hora e data por meio do protocolo NTP.

9. Detalhamento da Solução de Segurança

9.1. Site Central - Brasília

9.1.1. Topologia:
9.1.1.1. Devem ser instalados no site central de Brasília um par de firewalls do mesmo fabricante (a depender da solução escolhida, será utilizada solução Firewall NGFW contratada em 2020). Esses appliances atuarão em modo failover, no qual os appliances possuem a mesma ligação física na rede de dados e caso ocorra alguma falha com um dos appliances o outro assume o tráfego automaticamente.
9.1.2. Serviços habilitados:
9.1.2.1. Os NGFW devem possuir os seguintes licenciamentos:

- IPS – Serviço de *Intrusion Prevention System;*
- *Web Filtering* – Serviço de Filtro de conteúdo Web;
- *Application Control* – Serviço de Controle de Aplicação;
- VPN – Serviço de VPN, site to site ou VPN *cliente;*
- Antivírus.

9.1.2.2. Em tempo de operação, a critério da Funasa, novas features que estejam disponíveis poderão ser adicionadas através de abertura de chamado.
9.1.2.3. Ainda em tempo de implementação do projeto, será definida pela Funasa, a política deste serviço.

9.2. Sites Remotos:

9.2.1. Topologia das Superintendências Estaduais e Unidades Descentralizadas:
9.2.1.1. Para ligação física dos dois firewalls em alta disponibilidade, é de responsabilidade da Contratada fornecer todo e qualquer implemento necessário a sua perfeita instalação e funcionamento.
9.2.1.2. O default gateway da rede desses sites remotos deve ser o firewall a ser fornecido pela Contratada, que será responsável por encaminhar o tráfego para rede MPLS via rota estática ou para a Internet via rota default.

9.2.2. Serviços habilitados:

9.2.2.1. Serão habilitados os serviços de IPS, Antivirus, Antispyware e Webfilter. Deve ser implementada apenas uma política de webfilter. Inicialmente, não haverá autenticação de usuários, podendo vir a ser implementada a critério da Funasa.

10. Gerência dos NGFW

10.1. Os NGFW instalados fisicamente no site BSB e Sites Remotos do Grupo 1, serão gerenciados, de forma compartilhada, pela equipe técnica da Funasa e pela Contratada via link Internet, sendo de responsabilidade da Contratada o fornecimento dos endereços IP´s públicos a serem utilizados para gerência dos equipamentos.

10.2. Para efetuar o gerenciamento das configurações, será utilizada a solução de gerenciamento centralizado fornecida pela Contratada, que será instalada nas dependências da Funasa.

10.3. A solução de gerenciamento será responsável pelo recebimento dos logs do appliances físicos e geração de relatórios, nele serão criadas e aplicadas as políticas definidas pela Funasa para os equipamentos de segurança.

10.4. Os contatos de segurança serão centralizados no site de Brasília e estes possuirão acesso total ao sistema de gerência, às configurações, políticas, visualização de logs e obtenção de relatórios.

11. Instalação Piloto

11.1. A Instalação Piloto tem como objetivo mostrar para a Funasa que a rede contratada está em conformidade com o que foi projetado, atendendo plenamente as exigências estipuladas no Termo de Referência.

11.2. Objetiva a verificação do funcionamento, integração e interoperabilidade das tecnologias de conectividade e segurança, do ponto de vista da aplicação da arquitetura especificada no projeto executivo e entregue pela contratada, bem como a verificação do atendimento aos objetivos da rede.

11.3. A Contratada deverá encaminhar para a Funasa um Caderno de Testes, que apresente todas as rotinas técnicas para efetivos testes da solução. A Funasa deverá avaliar este Caderno de Teste quanto à possibilidade de execução e agendar uma data para a realização de todos os testes descritos.

11.4. Este teste será realizado com a ativação ou migração dos links principais e remotos indicados pela Funasa, devendo evidenciar a conectividade dos pontos indicados.

11.5. É de responsabilidade da Funasa o planejamento e execução de todos os testes relativos ao perfeito acesso e funcionamento das suas aplicações e sistemas de informação, garantindo que a rede fornecida atende aos requisitos especificados no TR.

12. Logs dos equipamentos fornecidos

12.1. Os logs serão mantidos pela solução de gerenciamento centralizado instalado no ambiente Datacenter da Funasa em Brasília, sendo a responsabilidade e a administração dos mesmos, compartilhada entre a equipe técnica da Funasa e a contratada. Fica critério da Funasa o armazenamento do backup e o tempo de retenção das informações de logs.

Anexo XI - Anexo XI - Locais de Instalação.pdf

Anexo XI – LOCAIS DE INSTALAÇÃO

SUPERINTENDÊNCIAS ESTADUAIS – CAPITAIS e Unidades Descentralizadas

Superintendência Estadual da Funasa no Acre (Suest – AC)

Rua Antônio da Rocha Viana, nº 1584 – Vila Ivonete – Rio Branco/AC CEP: 69900-526

Superintendência Estadual da Funasa em Alagoas (Suest – AL)

Av. Durval de Goes Monteiro, 6122 – Tabuleiro do Martins – Maceió/AL CEP: 57080-000

Superintendência Estadual da Funasa no Amapá (Suest – AP)

Rua Santos Dumont, nº 1484 – Santa Rita – Macapá/AP CEP: 68901-270

Superintendência Estadual da Funasa no Amazonas (Suest – AM)

Rua Oswaldo Cruz, s/nº, Bairro da Glória – Manaus/AM CEP: 69027-000

Superintendência Estadual da Funasa na Bahia (Suest – BA)

Av. Sete de Setembro, 2328 – Corredor da Vitória – Salvador/BA CEP: 40080-004

Unidades Descentralizadas BA:

Divisão de Engenharia de Saúde Pública e Saúde Ambiental Itabuna - DISEA-ITB - Avenida Félix Mendonça nº 56 H, Térreo, Bairro Goés Calmon CEP: 45.605-351 - Itabuna-BA

Divisão de Engenharia de Saúde Pública e Saúde Ambiental Barra - DISEA-BRR - Av. Getúlio Vargas nº 800 - Centro CEP 47.100-000 – Barra – BA.

Divisão de Engenharia de Saúde Pública e Saúde Ambiental Bom Jesus da Lapa - DISEA-BJL - Rua Oriente Médio, s/nº - Nossa Senhora da Soledade CEP 47.600-000 – Bom Jesus da Lapa – BA.

Divisão de Engenharia de Saúde Pública e Saúde Ambiental Jequié - DISEA-JQE - Prédio da Secretaria Municipal de Saúde, sala 25 - Rua Dom Pedro II, 88 - Centro CEP: 45.200-263 - Jequié/BA

Divisão de Engenharia de Saúde Pública e Saúde Ambiental Juazeiro - **DISEA**-JZR - Rua Carmela Dutra, nº 1020 - Centro CEP: 48.903-530 – Juazeiro – BA.

Divisão de Engenharia de Saúde Pública e Saúde Ambiental Feira de Santana – **DISEA** - FST - Rua Barão de Cotegipe nº 1520 – Kalilandia - CEP 44.002-135 – Feira de Santana – BA

Superintendência Estadual da Funasa no Ceará (Suest – CE)

Av. Santos Dumont, 1890 – Aldeota – Fortaleza/CE CEP: 60150-160

Unidade Descentralizada CE:

Setor de Transporte e Arquivo Desativado de Fortaleza - Av. Francisco Sá, Nº 1873 - Bairro Jacarecanga, Fortaleza –CE, CEP: 60010-450.

Depósito Central da Coordenação de Engenharia de Saúde Pública-COESP - Rua José Pereira de Abreu, Nº 54, Bairro São João, CEP 61946-090- Maranguape-Ceará.

Superintendência Estadual da Funasa no Espírito Santo (Suest – ES)

Rua Moacyr Strauch, 85, Praia do Canto – Vitória/ES CEP: 29055-630

Superintendência Estadual da Funasa em Goiás (Suest – GO)

Rua 82, nº 179 Setor Sul – Goiânia/GO CEP: 74083-010

Superintendência Estadual da Funasa no Maranhão (Suest – MA)

Rua do Apicum, 243 – Centro – São Luís/MA CEP: 65025-070

Unidade Descentralizada MA:

Prédio Anexo - Rua do Apicum, 241, Centro, São Luiz/MA – CEP 65025-070

Superintendência Estadual da Funasa em Minas Gerais (Suest – MG)

Rua Espírito Santo, nº 500, sala 607 – Centro – Belo Horizonte/MG CEP: 30160-030

Unidades Descentralizadas MG:

Almoxarifado / Setor de Transporte / Laboratório de análise da qualidade da água de Belo Horizonte - Rua Cid Rebelo Horta, 310 - João Pinheiro / Belo Horizonte –MG, CEP 30530-130.

SODEA/MCL de Minas Gerais - Av. Antônio Lafetá Rebelo, 332, bairro Santa Lúcia - Montes Claros/MG.

Superintendência Estadual da Funasa no Mato Grosso do Sul (Suest – MS)

Rua Barão de Melgaço, nº 379 – Centro – Campo Grande/MS CEP: 79002-080

Unidade Descentralizada MS:

Setor de Almoxarifado/Setor de Transporte de Campo Grande: Rua Américo Marques, 45, Vila Sobrinho, Campo Grande/MS – CEP 79.110-300

Superintendência Estadual da Funasa no Mato Grosso (Suest – MT)

Av. Getúlio Vargas, 967 – Centro Norte – Cuiabá/MT CEP: 78005-370

Superintendência Estadual da Funasa no Pará (Suest – PA)

Av. Visconde de Souza Franco, 616 – Reduto – Belém/PA CEP:66.053-000

Superintendência Estadual da Funasa na Paraíba (Suest – PB)

Rua Prof. Geraldo Von Shosten, 285 – Jaguaribe – João Pessoa/PB CEP: 58015-190

Superintendência Estadual da Funasa em Pernambuco (Suest – PE)

Av. Conselheiro Rosa e Silva, 1489 – Aflitos – Recife/PE CEP: 52050-020

Unidade Descentralizada PE:

Setor de Almoxarifado/Transporte de Recife - Rua 21 de Abril, 1385, Mustardinha, CEP: 50.820-000– Recife PE

Superintendência Estadual da Funasa no Paraná (Suest – PR)

Av. Cândido Lopes, 208, 8º andar, sala 804 – Centro – Curitiba/PR CEP: 80020-060

Unidades Descentralizadas PR:

Setor de Transporte de Curitiba - Rua Professor Basílio Ovídio da Costa, 639, Vila Izabel, Curitiba/PR, CEP 80320-100

SECAP Maringá: Rua Pioneiro Miguel Jordão Martines, 677 - Parque Industrial Mário Bulhões da Fonseca, Maringá/PR, CEP 87.065-660

Superintendência Estadual da Funasa no Piauí (Suest – PI)

Av. João XXIII, 1317 – Jockey Club – Teresina/PI CEP: 64049-010

Unidade Descentralizada PI:

Setor de Transporte de Teresina - Rua Professor Mauricio Silveira, 3317. Vila São Raimundo/Bairro São Raimundo, Teresina-PI CEP: 64075-035.

Superintendência Estadual da Funasa no Rio de Janeiro (Suest – RJ)

Rua Coelho e Castro, nº 6, 10º andar, Saúde – Rio de Janeiro/RJ CEP: 20081-060

Unidade Descentralizada RJ:

Barra de São João - URCQA Rua Santo Antonio, 155 Distrito de Barra de São João - Município de Casemiro de Abreu - RJ - CEP: 28.880 – 000

Superintendência Estadual da Funasa no Rio Grande do Norte (Suest – RN)

Av. Alexandrino de Alencar, nº 1402 – Tirol – Natal/RN CEP: 59015-350

Superintendência Estadual da Funasa no Rio Grande do Sul (Suest – RS) -

Av. Borges de Medeiros, nº 536, 11º andar – sala 1102 – Centro – Porto Alegre/RS CEP: 90020-022

Superintendência Estadual da Funasa em Rondônia (Suest – RO)

Rua Festejo 167 – Costa e Silva – Porto Velho/RO CEP: 78903-843

Superintendência Estadual da Funasa em Roraima (Suest – RR)

Av. Capitão Enê Garcez, nº 1874 – S. Francisco – Boa Vista/RR CEP: 69304-000

Superintendência Estadual da Funasa em Santa Catarina (Suest – SC)

Av. Max Schramm, nº 2179 – Estreito – Florianópolis/SC CEP: 88095-001

Superintendência Estadual da Funasa em São Paulo (Suest – SP)

Av. Prestes Maia, 733 - 21º andar - Centro Histórico de São Paulo - São Paulo/SP CEP: 01031-001

Superintendência Estadual da Funasa em Sergipe (Suest – SE)

Av. Tancredo Neves, nº 5425 – Jabotiana – Aracaju/SE CEP:49080-470

Superintendência Estadual da Funasa em Tocantins (Suest – TO)

Avenida Edifíco Homaidan - Quadra 104 Norte - Avenida LO 2, Lote 19 - Plano Diretor Norte - Palmas/TO - CEP: 77.006 - 022