

DIRETORIA DE ADMINISTRAÇÃO E GESTÃO - FUNAI

Estudo Técnico Preliminar 55/2025**1. Informações Básicas**

Número do processo: 08620.019559/2025-84

2. INTRODUÇÃO

2.1 Conforme previsto no artigo 11 da Instrução Normativa SGD/ME n. 94, de 23 de dezembro de 2022, o Estudo Técnico Preliminar da Contratação (ETP) compreende a definição e especificação das necessidades de negócio e tecnológicas, e dos requisitos necessários e suficientes à escolha da solução de TIC, contendo de forma detalhada, motivada e justificada, inclusive quanto à forma de cálculo, o quantitativo de bens e serviços necessários para a sua composição, e análise comparativa de soluções, que deve considerar, além do aspecto econômico, os aspectos qualitativos em termos de benefícios, para o alcance dos objetivos da contratação.

2.2 Na elaboração do ETP da Contratação, diversos aspectos são analisados em profundidade para que os gestores se certifiquem de que a necessidade da área de negócio, claramente definida, pode ser atendida, que os riscos identificados são gerenciáveis e que os resultados pretendidos com a contratação são compatíveis com preço estimado inicialmente. O ETP serve ainda como base para a elaboração do Termo de Referência (TR) ou Projeto Básico (PB), produzido somente se a contratação for considerada viável.

2.3 O Estudo Técnico Preliminar tem por finalidade identificar e analisar os cenários capazes de atender à demanda de contratação do serviço de INFOVIA, abrangendo infraestrutura de rede óptica metropolitana e os serviços complementares de link de internet e segurança, conforme registrado no Documento de Formalização da Demanda (DFD – SEI 09402062). Além disso, busca apresentar elementos que permitam demonstrar a viabilidade técnica e econômica das alternativas disponíveis, reunindo as informações necessárias para orientar o processo de contratação.

Referência: Inciso XI, do art. 2º e art. 11 da IN SGD/ME nº 94/2022.

3. Descrição da necessidade**3.1 VISÃO GERAL DA FUNDAÇÃO NACIONAL DOS POVOS INDÍGENAS - FUNAI E SEUS OBJETIVOS ESTRATÉGICOS:**

3.1.1 A Fundação Nacional dos Povos Indígenas (Funai) é o órgão indigenista oficial do Estado brasileiro, responsável por executar e monitorar a política indigenista nacional, com vistas à garantia dos direitos e da autonomia dos povos indígenas no Brasil. A Funai atua na proteção territorial, na promoção dos direitos sociais, culturais e linguísticos, bem como na gestão ambiental e territorial dos territórios indígenas, conforme estabelecido no seu Mapa Estratégico 2024–2027 e na legislação pertinente.

3.1.2. Para o cumprimento de suas missões institucionais e estratégicas, a Funai necessita de uma infraestrutura de Tecnologia da Informação e Comunicação (TIC) robusta e eficiente, que suporte suas diversas operações administrativas e finalísticas. Uma arquitetura moderna de ativos de rede é essencial para assegurar a execução das atividades voltadas à demarcação e proteção territorial, à defesa dos povos indígenas isolados e de recente contato, ao fortalecimento da cultura e dos direitos sociais indígenas e à gestão sustentável dos territórios indígenas.

3.1.3. No exercício de suas funções, a Funai atua em articulação com os órgãos e entidades da administração pública federal, estadual e municipal, além de dialogar com a sociedade civil e as próprias organizações indígenas, assegurando a transversalidade das políticas públicas e a efetividade dos direitos dos povos indígenas.

3.1.4. A missão institucional da Funai é “executar e monitorar a política indigenista com vistas à garantia dos direitos e da autonomia dos povos indígenas no Brasil”. Sua visão é “ser uma instituição fortalecida e reconhecida pelos povos indígenas e sociedade em geral, de excelência na execução e no monitoramento da política indigenista”.

Esses princípios orientam suas ações, alinhadas aos valores de protagonismo indígena, conhecimento indigenista, respeito à diversidade, atuação especializada, comprometimento, sustentabilidade, justiça e equidade.

3.1.5 O Mapa Estratégico da Funai 2024–2027 estabelece objetivos voltados à demarcação e proteção territorial, direitos sociais, direitos culturais e linguísticos, e gestão ambiental e territorial nos territórios indígenas, além de objetivos de suporte como regularizar a situação

patrimonial da Funai e aperfeiçoar e monitorar a gestão de contratação de bens e serviços. A infraestrutura tecnológica é um elemento habilitador para o alcance desses objetivos, promovendo conectividade, integração e eficiência administrativa.



Figura 1 - Mapa Estratégico

3.1.6. No contexto dos objetivos de suporte do Mapa Estratégico da Funai 2024–2027, destaca-se a importância de aperfeiçoar e monitorar a gestão, o que inclui a modernização da infraestrutura tecnológica e a adoção de soluções de TIC seguras de contratação de bens e serviços e eficientes, que sustentem os processos administrativos e finalísticos da política indigenista.

3.1.7. Para atingir tais objetivos de forma eficaz, é indispensável contar com recursos tecnológicos atualizados, capazes de prover informações estratégicas, apoiar a tomada de decisão e ampliar a capacidade institucional de gestão e monitoramento.

3.1.8. Um componente essencial para a execução dessas funções é a Coordenação-Geral de Tecnologia da Informação (CGTI), cuja competência está estabelecida no Regimento Interno da Funai. Compete à CGTI, entre outras atribuições:

- Elaborar, revisar e acompanhar a execução do PDTI, alinhado ao planejamento estratégico da Funai e às diretrizes do SISP;
- Implementar, divulgar e monitorar a POSIC, garantindo segurança e conformidade normativa;
- Definir e implementar estratégias voltadas à governança, otimização de recursos e transformação digital;
- Planejar, implementar, manter e aprimorar a infraestrutura tecnológica e os serviços de TI;
- Apoiar tecnicamente as unidades descentralizadas na gestão de TI, padronizando processos e difundindo boas práticas;
- Estabelecer e revisar normas de segurança da informação e uso de recursos computacionais;
- Demonstrar resultados financeiros e benefícios decorrentes dos investimentos em TI.

3.1.9 A estrutura da FUNAI é bastante ampla e complexa, possuindo diversas áreas de atuação que merecem tratamento diferenciado e proporcional às suas especificidades, tanto do ponto de vista de suas dimensões, quanto ao grau de sensibilidade e sigilo que as áreas necessitam para o desempenho de suas atividades, dentre essas encontra-se a Coordenação-Geral de Tecnologia da Informação - CGTI.

3.1.10 A CGTI da FUNAI vem observando, nos últimos anos, o aumento do fluxo de dados e o crescimento das demandas internas por soluções de Tecnologia da Informação. A análise do tráfego do link de internet, atualmente em período de degustação com velocidade de até 400 Mb/s — superior à velocidade contratada de 200 Mb/s — demonstra que, em diversos momentos, a utilização atinge esse limite ampliado, o que evidencia a saturação do link e dificulta a identificação precisa da demanda real. Esse cenário reforça a necessidade de soluções que proporcionem entregas tecnológicas rápidas, robustas, escaláveis, corporativas e alinhadas às alternativas disponíveis no mercado.

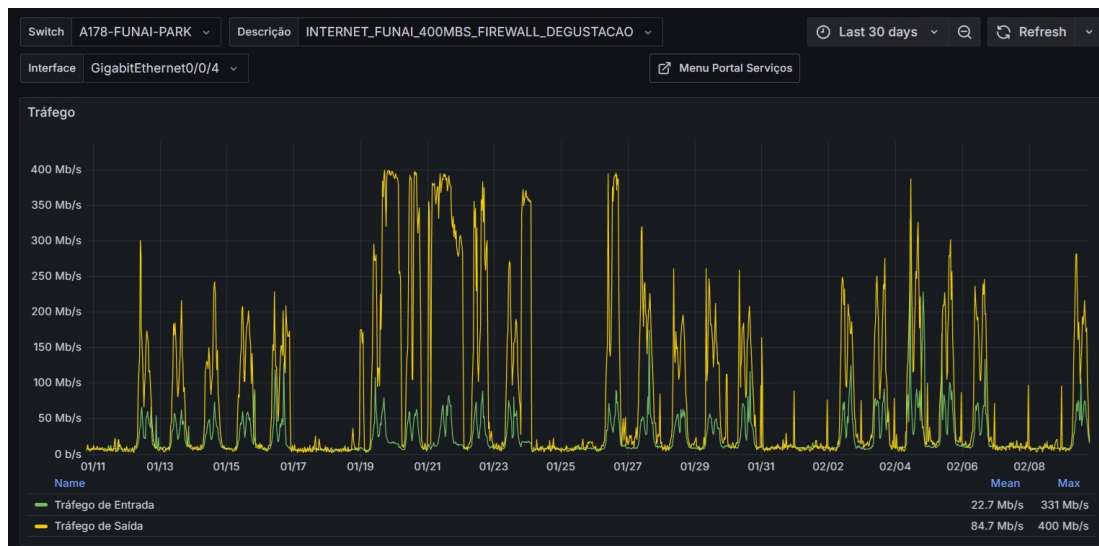


Figura 2 - Tráfego de entrada e saída do link de internet, com registros de saturação atingindo 400 Mb/s

3.1.11 Considerando, portanto, as necessidades da FUNAI junto a Coordenação-Geral de Tecnologia da Informação - CGTI, esta contratação se destina a permitir a continuidade da contratação de serviços especializados em tecnologia da informação e gerenciamento de conexões para esta Fundação, os quais sejam fornecidos por meio de uma infraestrutura de fibras ópticas, planejada para interconectar os clientes com alta largura de banda e com as mais modernas e inovadoras redes Metro *Ethernet* e, que sejam de uso exclusivo pelos órgãos e entidades públicas nas esferas federal e estadual, vinculados ao alcance geográfico da rede óptica, juntamente, com o serviço de segurança com proteção contra-ataques de tráfego maliciosos via *web* dessa Instituição.

3.2 SERVIÇO INFOVIA

3.2.1 Para dar cumprimento da missão institucional, suportar as atividades das áreas finalísticas e manter a prestação de serviços à sociedade, a infraestrutura de TI da FUNAI conta com equipamentos robustos (roteadores, switches e demais dispositivos), que depende dos links de comunicação entre os ativos de rede responsáveis pela troca de informações entre os dispositivos tecnológicos (computadores, notebooks, solução de HCI, switches, WiFi, entre outros) alocados nesta Fundação. Assim, faz-se necessária a contratação de link de comunicação baseado em infraestrutura de rede óptica metropolitana, com requisitos de disponibilidade, capacidade, segurança e gestão compatíveis com as necessidades institucionais.

3.2.2 A infraestrutura de comunicação destinada a suportar as demandas da FUNAI deve operar sobre rede óptica metropolitana voltada ao uso governamental, garantindo transmissão de dados com confiabilidade, continuidade, segurança e alta disponibilidade. Essa infraestrutura deve possibilitar comunicação eficiente entre unidades, oferecer e garantir ambiente seguro para troca de informações e contribuir para melhor desempenho dos serviços públicos associados ao fluxo de dados institucional. .

3.2.3 O serviço de conexão com banda larga pela Infovia varia de 10 Mbps a 10 Gbps, e garante infraestrutura suficiente para replicação de dados, hospedagem *web*, administração remota de ambientes, conexão site-to-site, além dos serviços de disponibilidade de acesso à *internet*. A solução poderá prever modelo de contratação escalonado, com melhor relação custobenefício para capacidades maiores. Também devem ser disponibilizados mecanismos de segurança como firewall, filtro de conteúdo, proteção contra-ataques de negação de serviço (antiDDoS) e sistema de prevenção de intrusões (IPS).

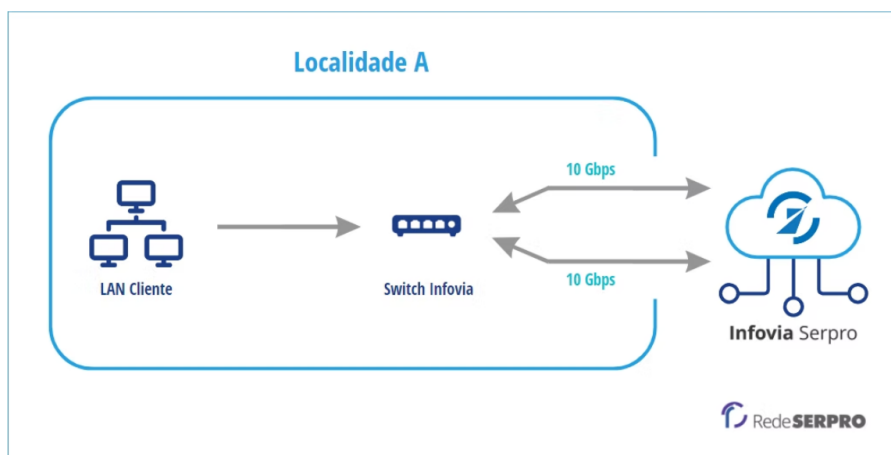


Figura 2 - INFOVIA - Topologia da Conexão Tipo 1. Disponibilizado em: <Loja Serpro/Infovia>, Acesso em: 30/06/2025

3.2.4 Atualmente, o serviço Infovia possui 77 (setenta e sete) órgãos da administração pública como clientes, conforme exposto na Relação de órgãos que utilizam a malha da Infovia, atualizada em 30/01/2025. Ressalta-se que não é comum a Administração Pública, no

âmbito da tecnologia da informação e comunicação, contratar serviços finalísticos com a iniciativa privada, sob pena de colocar em risco a autonomia ou até a própria segurança de suas informações, sendo recomendável a contratação de empresas públicas que possuam por finalidade a detenção dos dados e informações relacionadas ao objeto dos serviços a serem executados, com fulcro ao que dispõe o inciso IX do Artigo 75 da Lei 14.133, de 1º de abril de 2021.

[...]

Art. 75. É dispensável a licitação:

"IX - para a aquisição, por pessoa jurídica de direito público interno, de bens produzidos ou serviços prestados por órgão ou entidade que integrem a Administração Pública e que tenham sido criados para esse fim específico, desde que o preços contratado seja compatível com o praticado no mercado;"

[...]

3.2.5 Para atender as necessidades do órgão, o serviço de *link* de comunicação e a infraestrutura de cabeamentos, equipamentos específicos *switches*, *HCI*, roteadores, *workstations*, computadores, *notebooks*, licenças, serviço de nuvem, segurança de dados, se tornam imprescindíveis para a execução das atividades diárias dos setores que compõem esta Fundação. Assim, nos últimos quatro anos a Coordenação de Infraestrutura planejou e contratou diversas aquisições de equipamentos de rede e informática para atualização do parque computacional da FUNAI, além dos serviços de suporte de atendimento, manutenção, treinamento de soluções, segurança da informação e licenças de *software*.

3.2.6 Cabe ainda destacar que os serviços objetos da pretendida contratação geram ou trafegam informações sensíveis e estratégicas no ambiente interno da FUNAI e de várias áreas da Administração Pública Federal e, principalmente, das informações indigenistas no âmbito das aplicações/sistemas/serviços que são utilizados nas atividades administrativas desta Fundação, expostos na tabela I, abaixo:

Nº	ID (Chave primária)
1	AD Funai
2	Ajuda FUNAI
3	Ambiente de Backup
4	CADIN
5	CISCO UNIFIED CM
6	CMR
7	GATIC
8	Geoserver
9	GestioIP
10	GITLAB
11	Grafana
12	Huawei Esight
13	Impressoras
14	Intranet
15	iTop
16	Limesurvey
17	OCS Inventory
18	OTRS
19	PAPERCUT MF
20	PETRVUS
21	PNGATI
22	POLYWALL CGTIC
23	POLYWALL DPT
24	Portal Biblioteca
25	Portal CGGEO
26	Portal DPT
27	Rede WI-FI
28	SEI - Treinamento

29	SEI v3
30	SI3RC
31	SII
32	SISALDEIA
33	SISRH
34	Trellix Antispam
35	Trellix Anvírus
36	VSPHERE VMWARE
37	Windows FileServer
38	ZABBIX

Tabela I - Relação dos aplicativos/sistema disponibilizados pelos equipamentos de TIC alocados na sala segura da sede da FUNAI

3.2.7 Com esse cenário crescente da utilização dos recursos de infraestrutura de rede, evidencia-se o aumento constante do volume de dados trafegando no ambiente de rede, condição essa que torna necessário manter a estabilidade do funcionamento, prevenir as falhas, aplicar segurança e otimizar o uso desses recursos de forma a beneficiar os usuários internos e externos com a melhor qualidade de conexão.

3.2.8 Nesse contexto, a contratação proposta visa ampliar a capacidade de tráfego e a largura de banda, adequando-as às necessidades atuais. O contrato vigente, firmado em 2021, foi dimensionado com base em um cenário anterior e não atende mais às demandas dos hardwares, softwares e sistemas atualmente mantidos pela área de TIC, o que tem causado lentidão, falhas de comunicação e, por vezes, indisponibilidade de serviços.

3.2.9 Considerando a importância do tráfego de dados para a comunicação e o funcionamento das redes de computadores, a presente contratação tem por objetivo assegurar conectividade eficiente, segura, com alta disponibilidade e qualidade, mediante a ampliação do serviço de conexão à Internet atualmente contratado em 200 Mbps para um modelo escalável, contemplando os pacotes de 400 Mbps, 700 Mbps e 1 Gbps, bem como a possibilidade de contratação adicional de capacidade em Mbps de forma unitária, até o limite de 500 Mbps, conforme a necessidade do órgão, mediante pagamento proporcional à quantidade efetivamente solicitada, conforme a necessidade do órgão, mediante pagamento proporcional à quantidade efetivamente solicitada.

3.2.10 A execução dos serviços supramencionados na FUNAI, é realizado pelo Contrato Administrativo nº Contrato nº 136/2021 (SEI nº 3098641), com encerramento em 26/06/2026, não havendo possibilidade de nova prorrogação contratual.

3.2.11 Em vista disso, para assegurar a continuidade dos serviços necessários ao funcionamento interno e externo da Fundação, e considerando sua importância para o cumprimento dos objetivos institucionais e das ações previstas na área de tecnologia da informação, torna-se indispensável manter a prestação de serviços de comunicação de dados e de segurança da informação em níveis adequados. Esses serviços são fundamentais para o suporte às atividades finalísticas e para evitar riscos à autonomia, à segurança e à continuidade das operações realizadas por este órgão.

3.2.12 Destaca-se que os serviços da pretendida contratação são de natureza de prestação continuada, nos termos do inciso XV do Art. 6º da Lei n. 14.133, de abril de 2021, pautando-se na premissa que a contratação se baseia em serviços contratados pela Administração pública para a manutenção da atividade administrativa, decorrentes de necessidades permanentes ou prolongadas. E, ainda, enquadram-se nos pressupostos do Decreto n. 9.507, de 21 de setembro de 2018, constituindo-se em serviços auxiliares, instrumentais ou acessórios à área de competência legal da FUNAI, não inerentes às categorias funcionais abrangidas por seus respectivo plano de cargos.

3.2.13 Importa registrar também que os serviços a serem contratados compõem solução de TIC, para fins da Instrução Normativa SGD /ME n. 94, de 23 de dezembro de 2022, como exposto no item 1.6 do Anexo II dessa normativa.

4. Área requisitante

Área Requisitante	Responsável
COORDENAÇÃO DE INFRAESTRUTURA DE TECNOLOGIA DA INFORMAÇÃO - COINFRA	Bruno Alves de Lima

5. Necessidades de Negócio

ID	Principais necessidades de negócio
1	Garantir alta disponibilidade no acesso à rede ao link de internet
2	Garantir a confiabilidade, integridade, autoria e não repúdio das informações
3	Garantir a confidencialidade, integridade e segurança das informações disponibilizadas pelos diversos sistemas e aplicação da FUNAI
4	Garantir a infraestrutura e os recursos tecnológicos adequados às atividades da FUNAI;
5	Prover conectividade de alta capacidade: A solução contratada deve garantir uma infraestrutura de rede robusta e eficiente para assegurar a interconexão entre todas as unidades da FUNAI e outros órgãos da Administração Pública Federal, viabilizando o acesso seguro e ágil à internet, bem como a comunicação eficiente entre os servidores e sistemas desta Instituição.
6	Assegurar a continuidade dos serviços de conectividade: A solução deve garantir a continuidade e a disponibilidade ininterrupta dos serviços de conectividade de alta velocidade, atendendo às necessidades de tráfego de dados de alta criticidade e suportando as operações cotidianas da FUNAI, sem comprometer o desempenho ou a segurança da rede.
7	Garantir a segurança da comunicação e dos dados: A solução de conectividade deve incorporar mecanismos de segurança adequados para garantir a confidencialidade, integridade e disponibilidade das informações trafegadas na rede, atendendo aos requisitos de segurança cibernética e à proteção dos dados da FUNAI e dos cidadãos.
8	Prover suporte técnico e manutenção contínuos: A solução deve incluir serviços de suporte técnico e manutenção contínuos, assegurando que qualquer falha ou necessidade de atualização na infraestrutura de conectividade seja rapidamente resolvida, minimizando impactos nas operações da FUNAI.
9	Integrar soluções de redes privadas (VPNs) e locais (VLANs): A solução de conectividade deve possibilitar a implementação de redes privadas virtuais (VPNs) e redes locais de longa distância (VLANs), para garantir a segurança e eficiência no tráfego de dados entre as unidades da FUNAI e outros órgãos governamentais.
10	Prover acesso a sistemas e dados de forma eficiente: A conectividade deve permitir o acesso ágil e eficiente aos sistemas e bases de dados da FUNAI, facilitando o trabalho dos servidores públicos, o atendimento ao cidadão e a gestão das políticas públicas, além de promover a integração entre os diferentes sistemas governamentais.
11	Atender a requisitos de interoperabilidade: A solução contratada deve garantir que a FUNAI consiga interagir de forma eficiente com outros órgãos federais e entidades, possibilitando a troca de informações de forma ágil e segura, e promovendo a interoperabilidade entre as plataformas de TIC do governo federal.
12	Suporte para a digitalização de serviços públicos: A solução deve estar alinhada com a estratégia do governo digital, provendo a infraestrutura necessária para o desenvolvimento e a implementação de novos serviços digitais para a população, além de apoiar a transformação digital da FUNAI e a modernização dos processos administrativos internos.
13	Atender às exigências legais e normativas: A solução deve estar em conformidade com as legislações e normativas aplicáveis ao setor público, incluindo os requisitos de governança de TI, segurança da informação, privacidade de dados e transparência nas operações da Administração Pública.
14	Garantir proteção robusta para as aplicações e sistemas da FUNAI contra os mais avançados ataques.

Tabela II - Necessidades de Negócio

6. Necessidades Tecnológicas

Serviço Infovia	
1	Alta Capacidade de Banda: A necessidade de uma conexão de 10Gbps indica a demanda por uma infraestrutura capaz de suportar grandes volumes de dados, como aqueles gerados por aplicações de análise de dados, sistemas de gestão integrados e serviços online. Interoperabilidade com Outros Sistemas Capacidade de interagir com outras redes e sistemas externos, como a rede governamental.
2	Alta Disponibilidade: A infraestrutura deve ser projetada com redundância para garantir a continuidade dos serviços, mesmo em caso de falhas em componentes da rede. Isso é crucial para evitar interrupções nas operações da FUNAI.
3	Baixa Latência : Aplicações como videoconferência, transmissão de dados em tempo real e acesso a serviços em nuvem exigem baixa latência, ou seja, um tempo de resposta mínimo entre a origem e o destino dos dados.
4	Segurança: A proteção dos dados é fundamental para a FUNAI. A solução deve incluir mecanismos de segurança robustos, como <i>firewalls</i> , sistemas de detecção de intrusão e criptografia, para proteger a rede contra ataques cibernéticos.
5	Gerenciabilidade: A solução deve oferecer ferramentas de gerenciamento que permitam monitorar o desempenho da rede, identificar problemas e realizar ajustes de forma eficiente.
6	Escalabilidade : A infraestrutura deve ser capaz de se adaptar às futuras demandas da FUNAI, permitindo a expansão da capacidade e a adição de novos serviços.
7	Integração com Sistemas Existentes: A solução deve ser capaz de se integrar aos sistemas já existentes na FUNAI, como sistemas de gestão, bancos de dados e aplicações legadas.
8	Banda de conexão com o backbone: 10Gbps para a conexão principal
9	Relatórios gerenciais: Ferramentas para monitorar o desempenho da rede e gerar relatórios detalhados.
10	Atendimento técnico 24x7: Suporte técnico disponível 24 horas por dia, 7 dias por semana.
11	Gerenciamento da rede: Ferramentas para configurar, monitorar e administrar a rede.
12	Quantidade de VLANs: A capacidade de configurar até 25 VLANs (Virtual Local Area Network) indica a necessidade de segmentar a rede em múltiplas sub-redes, permitindo um maior controle sobre o tráfego de dados e a segurança da rede.
13	Fibra de acesso redundante: Redundância na infraestrutura física para aumentar a confiabilidade da conexão.

14	Prover disponibilidade de conexão de comunicação via satélite para as regionais com acesso limitado à conexão via terrestre dos serviços de <i>internet</i> .
----	---

Tabela III - Necessidades Tecnológicas

7. Demais requisitos necessários e suficientes à escolha da solução de TIC

ID	Requisitos de Arquitetura Tecnológica
1	A solução deverá ser compatível com as demandas previstas no PCA da FUNAI com vistas a facilitar e viabilizar a execução no Sistema PGC para o exercício de 2026;
Serviço de Infovia	
2	A solução deverá possibilitar que todo o tráfego seja analisado pelos serviços de segurança disponíveis em nuvem, tais como <i>WAF</i> e <i>AntiDDoS</i> e ter a aceleração do conteúdo dos sítios disponibilizados pelo cache.
3	Deverá prover proteção contra ataques cibernéticos aos sítios e aplicações web da Instituição assegurando a segurança das informações e a eficácia dos serviços de TIC por essa oferecidos na web, com qualidade, agilidade, confiabilidade e alta disponibilidade;
4	Deverá acelerar a entrega de conteúdo aos usuários de sítios e aplicações web.
5	Prover operação e suporte técnico especializado com níveis de serviço adequados quando da ocorrência de falhas de funcionamento da solução, bem como no apoio à realização de novas implementações e ajustes de configurações existentes visando ao funcionamento da solução customizada às necessidades de negócio da FUNAI.
6	Oferecer infraestrutura em rede óptica que interliga os órgãos da APF, Estadual ou Municipal, cuja topologia atual compreende pontos de concentração e distribuição interconectados por cabos óticos.
7	O projeto deve ser baseado em arquitetura de rede redundante, com caminhos alternativos de conectividade para garantir a alta disponibilidade e continuidade dos serviços, mesmo em caso de falhas de infraestrutura. A topologia da rede deverá ser planejada para suportar conexões de alta capacidade (mínimo de 1 Gbps), considerando a interligação das unidades da FUNAI com outros órgãos da Administração Pública via INFOVIA Brasília, utilizando links dedicados e segregação de tráfego por VLANs.
8	Serviço de conectividade - Tecnologia Metro Ethernet com suporte aos serviços <i>Multi Protocol Label Switching</i> (MPSL), <i>Traffic Engineering</i> (TE) e <i>Virtual Private LAN Service</i> (VPLS) com alta disponibilidade e velocidade em sua estrutura central.
9	Segurança: O projeto de rede deverá garantir a segurança da informação, implementando mecanismos como <i>firewalls</i> de última geração, VPNs para proteção de dados em trânsito e sistemas de monitoramento e detecção de intrusões (IDS/IPS), assegurando a proteção contra acessos não autorizados, ataques cibernéticos e outras ameaças. A autenticação multifatorial deverá ser aplicada para acesso à administração da infraestrutura de rede, garantindo maior proteção contra acessos indevidos.
10	Escalabilidade A solução deverá ser projetada com escalabilidade horizontal e vertical para suportar o aumento de tráfego de dados no futuro, considerando o crescimento das operações da FUNAI e a possível expansão do serviço de conectividade para outras unidades ou novos órgãos. A infraestrutura de rede deverá ser modular, permitindo o acréscimo de capacidade sem necessidade de substituição total de equipamentos, garantindo a continuidade do serviço durante a ampliação.

11	Qualidade e Desempenho A arquitetura deve assegurar que o serviço de conectividade ofereça alta qualidade com baixíssima latência, alta largura de banda e redundância ativa, para que a FUNAI possa operar sem interrupções ou perda de pacotes. O projeto deverá contemplar mecanismos de QoS (Quality of Service), para garantir o tratamento prioritário para serviços críticos e tráfego sensível à latência, como chamadas de voz e videoconferências.
12	O projeto deverá contemplar a utilização de endereçamento IPv4 e IPv6, atendendo às necessidades de compatibilidade com as infraestruturas de rede do governo federal e garantindo a escalabilidade para o futuro.
ID	Requisitos de Garantia e Manutenção
1	Durante a vigência contratual, ao SERPRO cabe a contratação e gerenciamento de recursos, a operação, gestão, garantia dos níveis de serviços e manutenção da infraestrutura ótica e dos equipamentos de rede.
2	As manutenções corretivas decorrentes de falhas na prestação de serviço por parte da CONTRATADA serão realizadas sem ônus para a FUNAI.
ID	Assistência Técnica
1	A contratada deverá fornecer suporte técnico especializado por meio de profissionais certificados na administração e suporte pelo próprio fabricante da solução.
ID	Requisitos Legais
1	O presente processo de contratação deve estar aderente à Constituição Federal, ao Decreto-Lei nº 200/1967 e à Lei nº 14.133/2021 (Lei de Licitações).
2	A referida contratação deve assegurar os princípios da Lei Geral de Proteção de Dados Pessoais (LGPD - Lei nº 13.709/2018), descritos no Artigo 6º. da Lei. Toda informação trafegada, por meio dos equipamentos de tecnologia da informação e comunicação, que fazem parte do objeto de contratação devem atender às exigências da Lei Geral de Proteção de Dados Pessoais.
3	Decreto nº 6.605, de 14 de outubro de 2008, que dispõe sobre o Comitê Gestor da Infra-Estrutura de Chaves Públicas Brasileira - CG ICP-Brasil, sua Secretaria-Executiva e sua Comissão Técnica Executiva - COTEC.
4	Decreto nº 11.984, de 09 de abril de 2024, Altera o Decreto nº 6.605, de 14 de outubro de 2009, que dispõe sobre o Comitê Gestor da Infraestrutura de Chaves Públicas Brasileira - CG ICP-Brasil.
5	Decreto nº 10.543, de 13 de novembro de 2020, que dispõe sobre o uso de assinaturas eletrônicas na administração pública federal e regulamenta o art. 5 da Lei nº 14.063, de 23 de setembro de 2020, quanto ao nível mínimo exigido para a assinatura eletrônica em interações com o ente público.
6	Instrução Normativa SGD/ME Nº 94, DE 23 DE DEZEMBRO DE 2022, 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.
7	Instrução Normativa SEGES /ME nº 65, de 07 de julho de 2021, que dispõe sobre o procedimento administrativo para a realização de pesquisa de preços para aquisição de bens e contratação de serviços em geral, no âmbito da administração pública federal direta, autárquica e fundacional.
8	Instrução Normativa SEGES/ME nº 67, de 08 de julho de 2021, que dispõe sobre a dispensa de licitação, na forma eletrônica, de que trata a Lei nº 14.133, de 1º de abril de 2021, e institui o Sistema de Dispensa Eletrônica, no âmbito da Administração Pública federal direta, autárquica e fundacional.

9	Instrução Normativa SEGES/ME nº 08, de 23 de março de 2023 - Altera a Instrução Normativa SEGES/ME nº 67, de 8 de julho de 2021, que dispõe sobre a dispensa de licitação, na forma eletrônica, de que trata a Lei nº 14.133, de 1º de abril de 2021, e institui o Sistema de Dispensa Eletrônica, no âmbito da Administração Pública federal direta, autárquica e fundacional.
ID	Requisitos de sustentabilidade da solução de TIC
1	Em atenção aos critérios de sustentabilidade, sobretudo como forma de observância à Lei n. 12.305, de 2 de agosto de 2010, que institui a Política Nacional de Resíduos Sólidos e o Decreto n. 7.746, de 5 de junho de 2012, que estabelece critérios e práticas para a promoção do desenvolvimento nacional sustentável nas contratações realizadas pela administração pública, procurou-se incluir requisitos mínimos nas especificações dos equipamentos que buscam garantir a observância da responsabilidade ambiental no âmbito da presente contratação.
2	A contratada deverá atender na execução do objeto os critérios de sustentabilidade ambiental contidas na Estratégia Federal de Desenvolvimento para o Brasil no período de 2020 a 2031 (EFD 2020-2031), conforme disposto no Decreto nº 10.531, de 26 de outubro de 2020, no que couber e no decreto nº 9.178, de 23 de outubro de 2017, no que couber.
ID	Requisitos de Segurança da Informação e Privacidade
1	Os serviços prestados deverão estar em conformidade com as leis, normas e diretrizes vigentes no âmbito da Administração Pública Federal, especialmente no que tange à Segurança da Informação e Comunicações (SIC) e à Lei Federal nº 13.709/2018 (LGPD).
2	Conformidade com Normas e Políticas: A CONTRATADA deverá adotar a Política de Segurança da Informação e Comunicações (POSIC) da FUNAI, além das normas federais relacionadas à segurança da informação.
3	Identificação e Confidencialidade: Os funcionários da CONTRATADA envolvidos na prestação de serviços deverão utilizar crachás de identificação. Todas as informações acessadas pela CONTRATADA durante a execução dos serviços deverão ser tratadas como confidenciais, sendo proibida sua reprodução, utilização ou divulgação sem a devida autorização.
4	Sigilo e Proteção de Dados: A CONTRATADA, seus representantes e colaboradores deverão garantir a confidencialidade de dados, informações, documentos e especificações técnicas adquiridas no desempenho das atividades. Além disso, a CONTRATADA deve implementar medidas que assegurem a disponibilidade, integridade, confidencialidade e autenticidade das informações tratadas
5	Proibição de Transferência de Dados: A CONTRATADA está proibida de obter, copiar ou transferir qualquer informação de propriedade da CONTRATANTE sem a devida autorização.
6	Cumprimento de Normas de Segurança: A CONTRATADA deverá seguir os procedimentos estabelecidos nas normas de segurança corporativa da FUNAI e da Administração Pública, em todos os eventos em que for necessária a presença de seus representantes nas dependências da CONTRATANTE.
7	Identificação de Equipamentos: Qualquer equipamento da CONTRATADA instalado nas dependências da CONTRATANTE deverá ser devidamente identificado, utilizando placas de controle patrimonial, selos de segurança ou outros meios adequados.

Tabela IV - Demais requisitos necessários e suficientes à escolha da solução de TIC

8. Estimativa da demanda - quantidade de bens e serviços

8.1 Atualmente a FUNAI possui vigente o Contrato Administrativo nº Contrato nº 136/2021 (3098641), cujo objeto é a contratação de serviços estratégicos e contínuos de Tecnologia da Informação e Comunicação - TIC, voltados, direta ou indiretamente, ao suporte necessário para as soluções estruturantes departamentais que atendem a FUNAI. Tais serviços consistem no atendimento especializado e nos serviços de infraestrutura de tecnologia da informação e comunicação - TIC, conforme o Projeto Básico vinculado à proposta, onde os serviços de Infovia, o qual foi firmado em 2021, contemplando inicialmente as seguintes descrição dos referidos serviços:

- Serviço Infovia do Contrato Administrativo nº136/2021 (Valores atuais reajustados):

Descrição	Unidade de Medida	Valor Unitário	Volume (Mensal)	Valor Mensal	Valor total Anual
Infovia - Conexão Tipo 1 a 1 Gbps	Parcela Mensal	R\$ 6.491,01	2	R\$ 12.982,02	R\$ 155.784,24
Acesso à Internet (200 Mbps)	Parcela Mensal	R\$ 15.626,49	1	R\$ 15.626,49	R\$ 187.517,88
Adicional de Segurança da Informação	Parcela Mensal	R\$ 19.265,06	1	R\$ 19.265,06	R\$ 231.180,72
Total Serviço Infovia				R\$47.873,57	R\$ 574.482,84

Tabela V - Custo/contrato atual - quantidade de bens e serviços

8.1.1 No contrato atualmente em vigor, a FUNAI dispõe de 01 (um) link de conexão básica tipo 1, no qual é disponibilizada uma porta física de 10/100/1000 Mbps no switch de acesso, bem como serviço de segurança básica mediante separação do tráfego do cliente em VLANs privadas. O serviço adicional de acesso à Internet possui faixa de 200 Mbps, sendo que a capacidade dos serviços de segurança da informação deve ser sempre equivalente à velocidade de conexão à Internet efetivamente contratada, de modo a garantir a proteção integral do tráfego de dados.

8.2 Considerando a estimativa da contratação atual, cuja vigência se encerra em 26/05/2026, constata-se a entrada de novos serviços e sistemas, a atualização dos ativos de rede e de infraestrutura, bem como o aumento do consumo de informações externas e internas deste órgão, o que torna a mensuração anterior ultrapassada e incapaz de acompanhar as crescentes demandas internas por soluções de Tecnologia da Informação da FUNAI. Nesse contexto, registra-se que o órgão se encontra em período de degustação, no qual o provedor vem entregando 400 Mbps pelo prazo de 85 dias, além da implantação do serviço de Wi-Fi institucional, que ampliará significativamente a demanda por conectividade, bem como da previsão de entrada do novo sistema SII. Destarte, torna-se necessário ampliar os volumes de conexão à Internet, de forma escalável, a fim de proporcionar entregas tecnológicas mais rápidas e com qualidade, bem como prover segurança aos serviços de armazenamento de dados e às soluções em nuvem no ambiente computacional desta Fundação.

8.2.1 Nesse sentido, para a presente contratação estima-se o serviço de INFOVIA no cenário a seguir:

Serviços de Conexão - INFOVIA			
Itens Faturáveis	Unidade de Medida	Quantidade Contratada / Mês	Meses estimados
Conexão Tipo 1 a 10 Gbps	Parcela Mensal	2	12
Serviço adicional de Conexão à Internet – Pacote de 400 Mbps	Parcela Mensal	1	12
Serviço adicional de Conexão à Internet – Pacote de 700 Mbps	Parcela Mensal	1	12
Serviço adicional de Conexão à Internet - Pacote de 1 Gbps	Parcela Mensal	1	12
Serviço adicional de Conexão à Internet - Excedente de Pacote de 1000 Mbps	mbps	500	12
Serviço Adicional de Segurança da Informação – Pacote 400 Mbps	Parcela Mensal	1	12
Serviço Adicional de Segurança da Informação – Pacote 700 Mbps	Parcela Mensal	1	12
Serviço Adicional de Segurança da Informação – Pacote 1 Gbps	Parcela Mensal	1	12
Serviço Adicional Segurança da Informação para Infovia - Excedente pacote 1000 Mbps	mbps	500	12

Tabela VI - Estimativa da demanda - quantidade de serviços

9. Levantamento de soluções

9.1 Baseado no presente estudo, será apresentado os tipos de cenários para as soluções dos serviços pretendidos nesta contratação, conforme segue:

9.2 Solução de Conectividade

9.2.1 Cenário 1 - Contratação de empresa privada para a prestação do serviço de conexão com banda larga.

9.2.1.1 Atualmente, o mercado privado possui grandes operadoras com uma vasta gama de provedores do serviço de conexão à *Internet* com banda larga via terrestre e satélite. Apesar do mercado privado ser dinâmico e proativo na adoção de novas tecnologias e soluções inovadoras oferecendo *links* dedicados com recursos e desempenho atualizados, há necessidade que as empresas sejam mais flexíveis na personalização dos serviços para atender às necessidades específicas dos seus clientes, condição essa que impede uma padronização na forma de prestação dos serviços.

9.2.1.2 As grandes operadoras nacionais como a Claro, Vivo (Telefônica Brasil), Oi, TIM e Algar Telecom, investem em redes redundantes, com múltiplas rotas de fibra e equipamentos de *backup*, para garantir a alta disponibilidade do serviço. A competitividade entre essas empresas privadas impulsiona a oferta de preços atraentes e planos mais flexíveis proporcionando opções que se ajustam melhor ao orçamento do órgão e as suas necessidades específicas de banda, IP fixo, redundância e SLAs (Service Level Agreements).

9.2.1.3 O segmento de empresas privadas que fornecem *internet* via satélite no Brasil também é amplo contando com as principais *Starlink*, *Hughesnet*, *Viasat*, Claro, Vivo e *InternetSat*. O mercado possui várias tecnologias na prestação desse serviço onde os fatores de localização da prestação do serviço, o tipo de uso, a franquia de dados e o segmento são considerados para dimensionar os produtos e os valores.

9.2.2 Cenário 2 - Contratação da empresa pública Telebrás para a prestação do serviço de conexão com banda larga.

9.2.2.1 A Telecomunicações Brasileiras S.A. - Telebras, é uma sociedade de economia mista, vinculada ao Ministério das Comunicações, que fornece acesso à *Internet* dedicado e exclusivo, com garantia da banda contratada, sem compartilhamentos com outros clientes. O serviço ofertado por essa empresa possui a arquitetura P2P, ligação ponto-a-ponto, com transmissão de dados suportada por fibras ópticas para disponibilizar circuitos dedicados, utilizando tecnologia *GigaEthernet*. Ideal para interligação de pontos de interesse dos clientes em todo território nacional, em áreas metropolitanas ou distribuídos regionalmente. A tecnologia de rede MPLS combina a inteligência do roteamento com o desempenho da comutação, realizando a convergência de redes para integras aplicações de dados, voz e vídeo, usando classes de serviço diferenciadas (COS) em uma única infraestrutura, sendo ideal para redes corporativas, escritórios comerciais ou órgãos de governo. E ainda, possui tecnologia que amplia drasticamente a quantidade de dados que podem ser transmitidos na rede de fibra. Utiliza diversos canais para transmitir múltiplos comprimentos de onda simultaneamente, multiplexando os sinais em uma única fibra óptica. Disponível em: <https://www.telebras.com.br/servicos/telebras-fibra> Acesso em: 18/10/2025.

9.2.2.2 O serviço de IP ofertado pela Telebras conta com as seguintes características:

- Velocidade simétrica para download e upload;
- Possibilidade de alocação de endereços de IP públicos;
- Escolha IPV4 e/ou IPV6 , e
- Anti-DDoS .

9.2.2.3 A Telebras também atua no fornecimento de conexão à *internet* via satélite no Brasil por meio do Satélite Geoestacionário de Defesa e Comunicações Estratégicas (SGDC).

9.2.3 Cenário 3 - Contratação da empresa pública SERPRO para a prestação do serviço de conexão com banda larga pela INFOVIA e seus serviços complementares de *Internet*, e conexão via satélite e serviço adicional de segurança.

9.2.3.1 A rede INFOVIA é exclusiva para órgãos e entidades públicas nas esferas federal e estadual vinculados ao alcance geográfico da rede óptica, onde exista disponibilidade de infraestrutura para conexão. Este serviço apresenta um alto desempenho e disponibilidade no âmbito metropolitano estabelecendo conexão com outros órgãos participantes da Rede Metropolitana.

9.2.3.2 Conforme exposto no item 3.2.3., o serviço de conexão básica conta com os seguintes atributos:

- Atendimento técnico 24 horas por dia e 7 dias por semana;
- Porta dedicada em *switch* de acesso;

- Segurança básica nível 2, por meio da separação do tráfego do cliente em VLANs privadas. A Segurança nível 2 está relacionada à camada 2 do Modelo OSI de redes, ou seja, segurança em nível de enlace. Em termos práticos, significa dizer que o tráfego dos clientes participantes das redes Infovias não se misturam, são segmentados em estruturas de nível 2 - VLANs, ou seja, túneis virtuais configurados fim a fim;
- Disponibilidade mensal de 99,9%, exceto para conexões tipo 2 e 6;
- Latência de até 50ms, mensurada a partir do cliente até o Serpro Regional Brasília;
- Taxa de erro menor que 1×10^{-8} ;
- Gerenciamento de falhas e indicadores de disponibilidade: compreende o tratamento de falhas e interrupções com a geração e acompanhamento de indicadores de disponibilidade;
- Relatórios Gerenciais de indicadores disponibilizados no portal do cliente.

9.2.3.3 No serviço de conexão à internet por meio de infovia, o SERPRO disponibiliza circuitos dedicados de acesso, cujas características variam conforme a largura de banda contratada, a unidade da Federação e a localização do ponto de acesso, em áreas urbanas ou interurbanas, utilizando infraestrutura terrestre de telecomunicações baseada predominantemente em fibra óptica, com emprego de tecnologias como MetroEthernet e MPLS, adequadas à interligação de unidades administrativas e ao tráfego seguro de dados em redes governamentais, com desempenho e disponibilidade compatíveis com aplicações corporativas. Disponível em: <https://www.serpro.gov.br/menu/noticias/noticias-2020/rede-serpro-conectividade-para-governo> Acesso em: 27/01/2026.

9.3 Solução de Segurança da Informação para proteção Web

9.3.1 Cenário 1 - Contratação de empresa privada para a prestação de serviço de proteção web.

9.3.1.1 Cenário do mercado privado de segurança da informação é vasto e conta com diversas empresas especializadas que oferecem uma gama ampla de serviços e produtos. Algumas das principais empresas atuantes no Brasil incluem *Sophos*, *Kaspersky*, *Fortinet*, *NetSecurity*, *ISH Tecnologia*, entre outras. Contratar esse tipo de serviço com empresas privadas pode oferecer a vantagem do ampla portfólio que incluem vários itens componentes da solução como exemplo, flexibilidade e customização, tecnologias de ponta, consultoria estratégicas.

9.3.1.2 A análise detalhada da necessidade de segurança e dos requisitos aos quais a organização está sujeita são referências para construir o ambiente mais adequado de proteção para o órgão, uma vez a abrangência desse serviço que vai além da proteção web como segurança de redes internas, *endpoints*, gerenciamento de identidades, consultoria estratégica em LGPD, dentre outros.

9.3.2 Cenário 2 - Contratação da empresa pública Telebras para a prestação de serviço de proteção web.

9.3.2.1 A Telebras oferece solução de proteção *Anti-DDoS*, contra os ataques de negação de serviço distribuídos, realizando ações preventivas e corretivas, com o auxílio do *software* e *hardware* necessário para a mitigação dos ataques em um centro de limpeza. Esse serviço é agregado à solução de conexão IP Telebras mais acessível ao mercado corporativo não sendo comercializado a parte.

9.3.3 Cenário 3 - Contratação da empresa pública SERPRO para a prestação de serviço de proteção web.

9.3.3.1 O Serpro possui uma plataforma de segurança em nuvem desenvolvida em parceria com a *Cloudflare*, voltado para a proteção de sites e aplicações web denominado. Uma das vantagens dessa solução é a possibilidade de ser contratada a parte das demais soluções de conectividade disponibilizados por essa empresa pública. O serviço oferece funcionalidades como *Web Application Firewall* (WAF), proteção contra *DDoS* (Negação de Serviço Distribuída) e CDN (Rede de Distribuição de Conteúdo), que visam garantir a disponibilidade e a segurança dos serviços *online*, com gerenciamento simplificado.

10. Análise comparativa de soluções

10.1 Mediante os cenários expostos no item 9 deste estudo, segue a análise preliminar das soluções identificadas. Ressalta-se que a análise dos cenários busca não apenas soluções, mas também serviços técnicos especializados agregados para manter de forma eficiente a estrutura tecnológica dessa instituição em pleno funcionamento e com um nível elevado de maturidade.

10.1.1 Cenário 1 - Contratação de empresa privada para a prestação do serviço de conexão com banda larga.

10.1.1.1 A Administração Pública neste cenário se torna dependente de um provedor externo para um serviço crítico, o que exige um planejamento robusto de redundância e contingência em caso de falha na prestação do serviço.

10.1.1.2 Destaca-se também que ao contratar o serviço com empresas privadas há dependência exclusiva onde o governo abre mão de parte do controle sobre uma infraestrutura de comunicação que pode ser considerada estratégica para a soberania nacional. Em situações de crise ou emergência, a prioridade ou a capacidade de atendimento pode ser diferente daquela oferecida por uma empresa pública focada nas necessidades do Estado.

10.1.1.3 Outra condição a ser observada numa contratação com empresa privada é o risco de descontinuidade dos serviços. Embora seja menos comum com grandes provedores, existe um risco maior de problemas de continuidade do serviço caso a empresa privada enfrente dificuldades operacionais ou até mesmo financeiras para manter os serviços contratados. Condição essa que torna evidente a paralisação dos serviços e, bem como a necessidade de um planejamento da contratação de forma emergencial elevando os gastos públicos previstos no planejamento adotado na primeira contratação.

10.1.1.4 Além dos pontos já mencionados, é importante destacar que as operadoras privadas não atendem a requisitos técnicos essenciais para a infraestrutura de comunicação utilizada pela Funai. Essas empresas trabalham em redes de transporte compartilhadas com diversos tipos de clientes, sem oferecer separação lógica dedicada exclusivamente a órgãos públicos. Nesse modelo, o tráfego da Funai circularia em uma malha comum, sem a garantia de isolamento em nível dois, o que é um elemento central para manter um ambiente seguro e compatível com as normas de segurança da informação adotadas pelo órgão.

10.1.1.5 Outro aspecto relevante é que as soluções privadas não incluem, de forma integrada, os mecanismos de proteção atualmente utilizados pela Funai, como filtragem de conteúdo, prevenção e detecção de intrusão e mitigação de ataques de negação de serviço. A contratação desses serviços de forma separada exigiria investimentos adicionais em equipamentos, contratos paralelos e maior esforço de administração, aumentando o custo total da solução e também a complexidade de gerenciamento.

10.1.1.6 Além disso, os acordos de nível de serviço oferecidos pelas operadoras privadas seguem padrões voltados ao mercado comercial, com disponibilidade e tempo de resposta inferiores àqueles exigidos pelo órgão para garantir o funcionamento contínuo dos sistemas corporativos. A ausência de suporte especializado para ambientes públicos e a dependência de infraestrutura que não integra a rede governamental utilizada por outros órgãos federais criam riscos adicionais de indisponibilidade e de inconsistência técnica na operação do ambiente.

10.1.1.7 Por esses motivos, ausência de isolamento lógico, falta de integração com os mecanismos de segurança já adotados pelo órgão, menor nível de disponibilidade e incompatibilidade com a estrutura governamental existente, a contratação de empresas privadas mostra-se tecnicamente inviável para atender às necessidades da Funai.

10.1.2 **Cenário 2 - Contratação da empresa pública Telebras para a prestação do serviço de conexão com banda larga.**

10.1.2.1 Os serviços prestados possuem características similares aos serviços prestados pelo SERPRO como infraestrutura robusta e abrangente com rede de fibra ótica, acesso dedicado à *internet* com banda exclusiva, sem compartilhamento com outros clientes, oferece endereço IP público, *Anti-DDoS*, segurança, soluções corporativas, conexão P2P, MPLS e foco no setor governamental e políticas públicas.

10.1.2.2 Ressalta-se que o ambiente disponibilizado por essa empresa não se trata de uma rede dedicada exclusiva ao governo, porém garante um ambiente seguro e controlado para a comunicação governamental.

10.1.2.3 Embora os serviços da Telebras apresentem uma estrutura sólida e contem com recursos utilizados no setor corporativo, é necessário observar que o modelo oferecido por essa empresa não corresponde à arquitetura atualmente adotada pela Funai. A solução em uso no órgão depende de uma malha de comunicação que funciona em um ambiente exclusivo para entidades públicas, com circuitos que operam em nível dois e permitem a criação de segmentos internos que se estendem de ponta a ponta dentro da rede governamental. Essa forma de operação não é reproduzida pela Telebras, que trabalha com um ambiente seguro, porém não dedicado e não isolado das demais conexões oferecidas pela empresa.

10.1.2.4 Outro ponto relevante é que a Funai utiliza serviços interligados ao backbone operado pelo Serpro, que integra conectividade, segurança, filtragem de tráfego, prevenção e detecção de intrusão e mecanismos de proteção contra ataques coordenados. Esse conjunto de funcionalidades atua de forma unificada e já está incorporado ao funcionamento dos sistemas internos do órgão. A Telebras não fornece essa integração nativa entre conectividade e segurança, o que tornaria necessária a contratação de recursos adicionais e a reconfiguração de toda a estrutura de comunicação do ambiente de produção.

10.1.2.5 Além disso, a substituição completa do provedor exigiria reendereço de serviços, revisão de rotas, alterações de regras de segurança, reconfiguração de equipamentos e validação de todos os sistemas que dependem da atual estrutura. Esse processo traria risco de indisponibilidade e aumento do esforço operacional, especialmente porque o ambiente abriga sistemas críticos que não podem sofrer interrupções. A Telebras poderia ser considerada para compor um cenário de redundância futura, mas não é adequada como alternativa principal para substituir a solução que já atende aos requisitos de isolamento, integração e continuidade necessários para o funcionamento regular da Funai.

10.1.3 Cenário 3 - Contratação da empresa pública SERPRO para a prestação do serviço de conexão com banda larga pela INFOVIA e seus serviços complementares de *Internet* e Segurança.

10.1.3.1 O serviço INFOVIA disponibilizado pela empresa pública SERPRO, apresenta as principais características dos serviços de banda larga:

- Serviço exclusivo para órgãos e entidades públicas;
- Possui estrutura física e lógica redundante para assegurar alta disponibilidade e resiliência, minimizando interrupções no serviço;
- Projetada para suportar elevado volume de tráfego de dados, essencial para as diversas aplicações e sistemas governamentais;
- Elevado nível de segurança oferecendo soluções como *firewall* contra acessos não autorizados, filtro de conteúdo para controle de acesso a determinados tipos de conteúdo na *internet*;
- *Anti-DDoS* contra ataques de negação de serviço distribuídos;
- IPS (Sistema de Prevenção de Intrusos), detecção e prevenção de atividades maliciosas na rede;
- Gerenciamento *online* que permite o acompanhamento e gestão do serviço pela *internet*;
- Serviços adicionais além do acesso à *internet*. A INFOVIA pode integrar-se a serviços de Nuvem e outras soluções de segurança da informação disponibilizado pelo SERPRO;
- Topologia flexível oferecendo diferentes combinações de enlaces de circuitos agregados para atender a diversas necessidades do contratante.

10.1.3.2 Embora existam diversas opções de conectividade no mercado, incluindo operadoras privadas e a Telebras, nenhuma delas atende, de forma completa, às necessidades específicas da FUNAI. As empresas privadas, ainda que ofereçam serviços de qualidade, não garantem o nível de segurança, estabilidade e controle necessários para o tratamento de informações sensíveis.

10.1.3.3 A Telebras, por sua vez, apesar de ser uma empresa pública, não se mostra adequada neste momento, pois toda a infraestrutura da FUNAI já está organizada e integrada ao ambiente atualmente utilizado.

10.1.3.4 Alterar esse ambiente exigiria mudanças extensas na rede, com risco de interrupções e impactos diretos em atividades essenciais. Assim, a manutenção da solução atual se apresenta como a alternativa mais segura para preservar a continuidade dos serviços, proteger dados sensíveis e assegurar o funcionamento regular da Fundação.

Solução de Segurança da Informação para proteção Web

10.1.6 Cenário 1 - Contratação de empresa privada para a prestação de serviço de proteção web.

10.1.6.1 Geralmente, as empresas prestadoras desse serviço oferecem pacotes de segurança que podem incluir os serviços de segurança de *endpoint*, segurança de rede e aplicações, serviços de gerenciados de segurança (MSSP), SOCs terceirizados. O público alvo prioritário das empresas privadas é amplo e envolve o setor público e o privado.

10.1.6.2 Embora as empresas privadas ofereçam soluções variadas de segurança, esse modelo não apresenta os elementos técnicos necessários para atender à realidade da Funai. Essas empresas atuam por meio de infraestruturas compartilhadas que atendem diversos segmentos, o que impede a garantia de isolamento pleno do tráfego e dificulta o controle sobre todo o fluxo de informações que envolve os sistemas do órgão. Nesse tipo de ambiente, parte da proteção teria de ser contratada separadamente e configurada de forma manual, gerando maior dependência operacional e reduzindo a capacidade de reação diante de incidentes.

10.1.6.3 Além disso, a ausência de integração direta entre a conectividade utilizada pela Funai e os sistemas das empresas privadas compromete o desempenho das camadas de segurança necessárias para proteger as aplicações que operam no ecossistema institucional. Como o tratamento de tráfego, os registros de eventos e os mecanismos de mitigação não funcionam de forma unificada, a Funai acabaria distribuindo responsabilidades entre diferentes fornecedores, o que amplia riscos, aumenta a complexidade de gestão e pode gerar inconsistências no atendimento de incidentes críticos.

10.1.6.4 Por fim, o atendimento prestado por fornecedores privados segue padrões voltados ao mercado comercial, com práticas e

prioridades que não contemplam as exigências de continuidade, rastreabilidade e governança pública. A falta de integração com a estrutura governamental já utilizada pelo órgão representa uma limitação importante, tornando esse cenário tecnicamente inadequado para suportar uma estratégia de segurança que demanda coerência entre conectividade e proteção de aplicações.

10.1.7 Cenário 2 - Contratação da empresa pública Telebras para a prestação de serviço de proteção web.

10.1.7.1 Os serviços de proteção contra ataques de negação (Anti-DDoS) oferecidos pela Telebras são disponibilizados como benefício na contratação de internet com banda dedicada. A proposta da Telebras informa que os serviços de IP contemplam mecanismos de mitigação de ataques de negação em três abordagens: detecção, análise e mitigação. As ferramentas são capazes de mitigar tanto ataques por inundação (ICMP Flood, UDP Flood, TCP SYN Flood), quanto ataques por exploração de protocolos (HTTP GET Flooding e DNS Reflection Attacks). Esses serviços são similares aos ofertados pelo SERPRO, contudo, o pacote de serviços de segurança disponibilizado pelo SERPRO apresenta maior abrangência e robustez, sendo concebido para uso agregado e indissociável à proteção da rede Infovia.

10.1.7.2 Embora a Telebras ofereça mitigação contra-ataques de negação de serviço, sua solução não contempla todos os mecanismos necessários para proteger as aplicações e serviços utilizados pela Funai. A proteção fornecida está vinculada ao tráfego que passa exclusivamente pelo link contratado, o que não cobre aplicações hospedadas em ambiente Serpro ou serviços que dependem de camadas de segurança mais avançadas, como inspeção detalhada de requisições, controle de comportamento e análise de padrões específicos das aplicações institucionais.

10.1.7.3 Além disso, a Telebras não oferece uma solução completa equivalente àquelas que agregam firewall de aplicação, proteção de DNS, aceleração de conteúdo e mecanismos integrados de monitoramento. Esses serviços são fundamentais para assegurar o desempenho e a segurança dos sistemas que operam no ambiente do órgão, especialmente aqueles publicados para acesso público ou que se conectam a outros sistemas da administração federal. A ausência dessa integração significa que a Funai teria de adotar recursos adicionais para completar as camadas de segurança necessárias.

10.1.7.4 Outro ponto relevante é que a proteção da Telebras não está alinhada à estrutura já utilizada pela Funai, que funciona integrada à rede Infovia e ao conjunto de serviços de segurança oferecidos pelo Serpro. Essa falta de alinhamento impede a continuidade dos padrões de proteção já instalados e aumentaria a necessidade de adaptações, reconfigurações e validações adicionais, criando risco operacional e complicando o gerenciamento do ambiente. Em razão dessas limitações, a solução oferecida pela Telebras não atende plenamente às necessidades de segurança do órgão no contexto atual.

10.1.8 Cenário 3 - Contratação da empresa pública SERPRO para a prestação de serviço de proteção web.

10.1.8.1 O serviço Govshield do SERPRO se trata de um produto específico de segurança web, além dos disponibilizados como adicionais nos serviços de conectividades.

10.1.8.2 No SERPRO o serviço Govshield possui como principais funcionalidades: Web Application Firewall (WAF); Proteção contra DDoS ; Central de segurança 24/7 (SOC); Aceleração de conteúdo digital (CDN) e Proteção de DNS (Full DNS), e, bem como traz como vantagens adicionais os serviços: **Security Operations Center - SOC**: grupo multidisciplinar responsável pela coordenação e gerenciamento dos incidentes de segurança, formado pelas equipes de 1º, 2º e 3º nível, atuando na prevenção de ataques cibernéticos e proteção dos serviços de governo sob gestão do SERPRO. Os serviços prestados pelo SOC ao GovShield devem ser de aprimoramento de detecção (coleta de logs e monitoração de segurança) e proatividade de bloqueio, por meio do reputation e, a **Central de Serviço Serpro - CSS** - será disponibilizado pelo SERPRO serviço de atendimento remoto disponível para registro de acionamento de possíveis falhas identificadas na execução dos serviços, com atendimento ao usuário, realizado de forma ininterrupta por 24 (vinte e quatro) horas por dia e 7 (sete) dias por semana. O acionamento será via Central de Serviços SERPRO (CSS). Serão criadas ofertas na ferramenta de workflow do SERPRO, e criados os grupos técnicos de atendimento. Os acionamentos que não forem solucionados pela CSS serão repassados para o gestor de solução, cujos prazos, por tipo de problema, serão estabelecidos em conjunto com o cliente. Disponível em: <https://centraldeajuda.serpro.gov.br/govshield/faq/>. Acesso em: 20/01/2026.

10.2 Examina-se nesta seção, para cada solução, os aspectos previstos na IN SGD/ME n. 94/2022 que devem ser avaliados em uma contratação de TIC:

Requisito	Cenário	Sim	Não	Não se aplica
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública.	Infovia			
	1	X		
	2	X		
	3	X		
	Segurança			
	1	X		
	2	X		

	3	X		
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Infovia			
	1			X
	2			X
	3			X
	Segurança			
	1			X
	2			X
	3			X
	A Solução é composta por software livre ou software público? (quando se tratar de software)	Infovia		
1				X
2				X
3				X
Segurança				
1				X
2				X
3				X
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?		Infovia		
	1	X		
	2	X		
	3	X		
	Segurança			
	1		X	
	2	X		
	3	X		
	A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Infovia		
1				X
2				X
3		X		
Segurança				
1				X
2				X
3				X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o		Infovia		
	1			X
	2			X
	3			X

objetivo da solução abranger documentos arquivísticos)	Segurança			
	1			X
	2			X
	3			X

Tabela VII - Comparativo dos cenários segundo os aspectos previstos na IN SGD/ME n. 94/2022

10.3 Com base na análise de comparação das soluções apresentadas, os cenários 3 das soluções de Infovia/Link e Segurança são considerados viáveis do ponto de vista técnico, um vez que atendem aos padrões técnicos e de qualidade dos serviços a serem prestados sem gerar um custo elevado, se for considerado que a estrutura do o serviço Infovia faz parte da infraestrutura já alocada no ambiente de rede desta Fundação. Sendo assim, cabe considerar a necessidade de desinvestimentos em ferramentas nas soluções já contratadas, além do grande esforço em alterar configurações de segurança e padrões realizados na entrada dos serviços do SERPRO no ambiente tecnológico da FUNAI.

11. Registro de soluções consideradas inviáveis

11.1 Cenário 1 - Contratação de empresa privada para a prestação do serviço de conexão com banda larga.

11.1.1 Considerando que o serviço de conexão à internet se trata de um serviço finalístico no âmbito do órgão, ressalta-se que a contratação desse serviço junto à iniciativa privada pode colocar em risco a autonomia administrativa ou até a própria segurança de suas informações e dados críticos, sendo recomendável a contratação de empresas públicas que possuam por finalidade a detenção dos dados e informações relacionadas ao objeto dos serviços a serem executados, com fulcro no inciso IX do art. 75.

11.1.2 Assim, este cenário é considerado inviável.

11.2 Cenário 2 - Contratação da empresa pública Telebras para a prestação do serviço de conexão com banda larga e via satélite.

11.2.1 Apesar da Telebras ser uma empresa pública, destaca-se que algumas condições que não favorecem, para o presente momento, pode-se pensar a Telebrás como sendo um possível link redundante dentro de um outro contrato para atender a FUNAI. Contudo, neste contexto, a troca de uma empresa fornecedora por outra, uma vez as dificuldades técnicas que são um dos maiores entreves, tendo em vista que a infraestrutura e os sistemas da Funai já estão integrados com a solução disponível pelo atual contrato com o Serpro, conforme alguns exemplos elencados a seguir:

- Necessidade de realizar a compatibilidade e reconfiguração de equipamentos. Alterar a empresa provedora do serviço forçaria a reconfiguração de vários equipamentos que integram a rede do órgão. Isso pode envolver mudanças de *firmware*, *drivers*, ou até a compra de novos módulos de interface, gerando custos adicionais e tempo de inatividade;
- Interrupção ou indisponibilidade de serviços essenciais. O órgão não pode simplesmente "ficar *offline*" por um dia pela questão dos serviços críticos à população e manter as operações internas que dependem diretamente da conectividade. Garantir uma transição quase imperceptível exige planejamento de contingência robusto, como a manutenção de um *link* secundário (um *backup*) ativo durante a troca das contratadas. No entanto, mesmo com *backup*, a migração dos sistemas e serviços para o novo *link* principal ainda pode apresentar falhas inesperadas, como problemas de rota ou latência, afetando o desempenho das aplicações.
- Segurança da informação. A transição de provedor pode introduzir novas vulnerabilidades se não for feita com extremo cuidado. É preciso garantir que o novo *link* de *internet* seja tão seguro, ou mais seguro, que o anterior. Isso significa reavaliar e reconfigurar *firewalls*, sistemas de prevenção de intrusão (IPS/IDS), políticas de acesso à rede e o gerenciamento de credenciais de acesso, para evitar que o período de transição se torne uma janela para ataques cibernéticos.

11.2.2 Nesse sentido, as dificuldades técnicas em trocar um provedor de *internet* envolvem uma reengenharia significativa da rede, a gestão de interrupções críticas e a garantia contínua da segurança dos dados e serviços, demandando um planejamento meticuloso e uma equipe de TI altamente capacitada. Este cenário é possível para uma futura contratação, pensando em manter um link redundante, mas não como um link para substituição do atual.

11.2.3 Assim, este cenário é considerado inviável.

Solução de Segurança da Informação para proteção Web

11.3 Cenário 1 - Contratação de empresa privada para a prestação de serviço de proteção web.

11.3.1 Ressalta-se que nesse cenário há risco de conformidade e soberania de Dados quando se trata de atendimento aos requisitos regulatórios como a Lei Geral de Proteção de Dados - LGPD. É essencial verificar se o provedor está em total conformidade com as leis e regulamentações de proteção de dados aplicáveis (LGPD no Brasil). A falha do provedor em cumprir as normas pode impactar a própria conformidade do órgão contratante.

11.3.2 Assim, este cenário é considerado inviável.

11.4 Cenário 2 - Contratação da empresa pública Telebras para a prestação de serviço de proteção web.

11.4.1 Para este cenário, é importante considerar que para ter este serviço pela Telebras seria necessário realizar a troca do provedor de acesso à internet, uma vez que a disponibilidade dessa segurança da informação é serviço adicional da aquisição do link dedicado. Assim, como não se trata de um serviço específico de proteção aos sistemas e aplicação web, e, ainda, considerando que não inclui funcionalidades agregadas para o serviço de segurança da informação importantes se comparado ao serviços adicionais prestados pelo SERPRO, este cenário é considerado inviável.

12. Análise comparativa de custos (TCO)

12.1. A análise comparativa de soluções considerou não apenas o custo de aquisição imediata, mas o **Custo Total de Propriedade (TCO)** ao longo de 12 meses, ponderando os benefícios da integração nativa entre conectividade e segurança cibernética (WAF/Anti-DDoS) oferecida pela Infovia Brasília.

12.2. A metodologia de aferição de preços seguiu rigorosamente o disposto na **Instrução Normativa SEGES/ME nº 65/2021** e na **IN SGD /ME nº 94/2022**, priorizando a consulta a contratações similares no setor público e dados do Painel de Preços, garantindo a compatibilidade com os preços praticados no mercado.

12.3. Conforme detalhado na **Nota Técnica nº 4/Seinfra (SEI nº 09641843)**, que subsidia este estudo, a análise documental de contratos vigentes de órgãos como CGU, Ministério da Saúde, STF e ICMBio ratifica que os valores referenciais adotados estão alinhados a média praticada pela Administração Pública Federal para objetos idênticos.

12.4. A opção pela solução da Infovia Brasília apresenta-se como a mais vantajosa economicamente (Cenário 3), pois elimina custos indiretos com suporte especializado de terceiros, hardware adicional e licenças de segurança que seriam necessários em soluções de mercado comum, consolidando uma economia estimada de escala por meio do uso da infraestrutura governamental já estabelecida.

12.5. Os quadros detalhados com a relação de contratações similares, números de contratos, vigências e memórias de cálculo unitárias encontram-se integralmente disponíveis na supracitada **Nota Técnica**, evitando-se a duplicidade de informações neste documento e garantindo a celeridade na análise processual.

12.6. Para validação da economicidade e determinação da base de cálculo do TCO, realizou-se o confronto direto entre os preços de referência da pesquisa de mercado, consolidados na Nota Técnica nº 4/2026, e a proposta comercial apresentada pelo SERPRO. O resultado dessa análise comparativa, que demonstra o pleno alinhamento e a vantagem econômica da solução ofertada, é detalhado no quadro abaixo:

Item	Descrição	Valor Unitário Nota técnica 04	Valor Unitário PROPOSTA SERPRO	Economia Estimada (%)
1	INFOVIA – Conexão Tipo 1 a 10 Gbps	R\$ 7.960,00	R\$ 7.960,00	0,00% (Alinhado)
2	INFOVIA – Serviço adicional de Internet – Pacote 400 Mbps	R\$ 12.000,00	R\$ 12.000,00	0,00% (Alinhado)
3	INFOVIA – Serviço adicional de Internet – Pacote 700 Mbps	R\$ 15.400,00	R\$ 15.400,00	0,00% (Alinhado)
4	INFOVIA – Serviço adicional de Internet – Pacote 1 Gbps	R\$ 16.000,00	R\$ 16.000,00	0,00% (Alinhado)
5	INFOVIA – Adicional Internet – Excedente 1000 Mbps	R\$ 16,00	R\$ 16,00	0,00% (Alinhado)
6	INFOVIA – Adicional Segurança – Pacote 400 Mbps	R\$ 38.532,00	R\$ 24.096,00	37,46%
7	INFOVIA – Adicional Segurança – Pacote 700 Mbps	R\$ 33.382,00	R\$ 33.382,00	0,00% (Alinhado)
8	INFOVIA – Adicional Segurança – Pacote 1 Gbps	R\$ 38.625,00	R\$ 38.625,00	0,00% (Alinhado)
9	INFOVIA – Adicional Segurança – Excedente 1000 Mbps	R\$ 38,63	R\$ 38,63	0,00% (Alinhado)
Soma dos Preços Unitários		R\$ 161.953,63	R\$ 147.517,63	8,91%

Tabela VIII - Comparativo entre os Preços de Referência da Pesquisa de Mercado (Nota Técnica nº 4/2026) e a Proposta Comercial do SERPRO.

12.7. Como se observa, a proposta do SERPRO apresenta valores iguais ou significativamente inferiores à mediana de mercado, com destaque para o Item 6 (Segurança - 400 Mbps), que apresenta uma economia de 24,8% em relação ao preço referencial apurado.

12.8. Diante do exposto, os valores da proposta do SERPRO serão utilizados como base para o cálculo do TCO real da contratação, enquanto os valores da Nota Técnica nº 4/2026 permanecem como o Preço Máximo Admissível, garantindo a segurança jurídica do teto orçamentário.

12.9 A estimativa de preço foi obtida por meio de consulta ao Portal Nacional de Contratações Públicas - PNCP - GOV.

12.9.1 Para a elaboração do cálculo do custo total de propriedade, foi considerado a variação do Índice de Custos de Tecnologia da Informação e Comunicação - ICTI, dos últimos 12 (doze) meses, referência ao último período de divulgação outubro de 2025, que corresponde a 3,57% (três virgula cinquenta e sete por cento), para um contrato com vigência de 12 (doze) meses, podendo ser prorrogado para até 10 (dez) anos. Para fins de estimativa do Custo Total de Propriedade (TCO), adotou-se como velocidade de referência o link de 700 Mbps, por representar um cenário intermediário e compatível com a demanda média projetada ao longo da vigência contratual, considerando a natureza escalável da contratação, que permite a variação entre as velocidades de 400 Mbps, 700 Mbps e 1 Gbps, conforme a necessidade do órgão.

O Índice de Custo da Tecnologia da Informação (ICTI), calculado pelo Ipea, apresentou taxa de variação de -0,21% em outubro de 2025, situando-se 0,57 ponto percentual (p.p.) abaixo da taxa registrada no mês anterior. Na comparação com o mesmo mês de 2024, a variação foi 0,84 p.p. menor. Com a incorporação desse resultado, o ICTI acumula uma variação de 3,57% nos últimos doze meses.

ICTI versus índices amplos de preços de outras fontes (out./2025)
(Variação, em %)

	ICTI	IPCA	IGP-M	IPA-EP
	Ipea	IBGE	FGV	FGV
Outubro de 2025	-0,21	0,09	-0,36	-0,13
Outubro de 2024	0,63	0,56	1,52	2,01
Acumulado em 2025	2,48	3,73	-1,30	-3,53
Acumulado em doze meses	3,57	4,68	0,92	-0,87

Fonte: Ipea, IBGE e FGV.
Elaboração: Grupo de Conjuntura da Diretoria de Estudos e Políticas Macroeconômicas (Dimac) do Ipea.

Figura 3 - ICTI versus índices de preços de outras fontes

12.9.2 Neste demonstrativo abaixo, o referido índice foi aplicado para o primeiro e um possível segundo e terceiro ano de vigência contratual, caso tenha renovação, conforme demonstrado a seguir:

Grupo	Descrição	Estimativa dos valores a serem praticados durante a vigência contratual, considerando o índice de 3,57% anual				
1	Infovia + Segurança	Ano 1	Ano 2	Ano 3	Ano 4	Ano 5
		R\$ 776.424,00	R\$ 804.142,34	R\$ 832.850,22	R\$ 862.582,97	R\$ 893.377,18
Custo Total (5 Anos)		R\$ 4.169.376,71				

Tabela IX - Estimativa dos valores a serem praticados durante a vigência contratual

12.9.3 Consideradas as premissas estabelecidas no item 12.9.1 e a aplicação do índice de reajuste conforme demonstrado no item 12.9.2, o Custo Total de Propriedade (TCO) dos serviços a serem contratados, calculado com base na velocidade de referência de 700 Mbps, é estimado em R\$ 4.169.376,71(quatro milhões, cento e sessenta e nove mil, trezentos e setenta e seis reais e setenta e um centavos.) , para o período de 60 (sessenta) meses, valor utilizado exclusivamente para fins de planejamento e condicionado à efetiva utilização dos serviços ao longo da vigência contratual.

12.10 Após a definição da composição da solução de tecnologia da informação a ser adquirida, conforme registrado nos itens 10 e 11 deste estudo, verifica-se a necessidade da realização dos procedimentos para a estimativa de custos para a aquisição da solução.

12.10.1 A comparação de preços e a justificativa da viabilidade financeira demonstram que a solução a ser contratada junto ao SERPRO está dentro dos parâmetros dos valores de mercado e atendem aos requisitos de eficácia e economicidade previstos pela legislação,

13. Descrição da solução de TIC a ser contratada

13.1 Descrição Geral do serviço Infovia Brasília

13.1.1 O serviço INFOVIA-DF funciona sobre fibras óticas e infraestrutura de propriedade do Ministério da Gestão e Inovação em Serviços Públicos (MGI) em um ambiente operado pelo SERPRO. Trata-se de um serviço de conexão de clientes ao SERPRO através de uma infraestrutura de fibras óticas. Planejada para interconectar os clientes com alta largura de banda, segurança e ausência de custos relacionados a aluguel de meios de conexão e operadoras locais de telecomunicação. As mais modernas e inovadoras tecnologias construtivas são utilizadas na Infovia que são redes Metro Ethernet. Este serviço permite ao Demandante beneficiar-se de alto desempenho e disponibilidade no âmbito metropolitano. São exemplos desse tipo de aplicação o acesso ao Datacenter do Serpro Regional Brasília para hospedagem de dados e o estabelecimento de conexão com outro órgão participante da Rede Metropolitana. Exclusivo para órgãos e entidades públicas nas esferas federal e estadual vinculados ao alcance geográfico da rede óptica, onde exista disponibilidade de infraestrutura para conexão. No caso de não haver disponibilidade de infraestrutura próxima ao local do órgão, e exista viabilidade técnica para expansão do backbone ou acesso, o órgão interessado poderá arcar com esta expansão, às suas expensas.

13.1.2 A rede Infovia Brasília surgiu em 2004 da parceria da antiga Secretaria de Logística e Tecnologia da Informação (SLTI/MP), atual Secretaria de Governo Digital (SGD/ME), e do SERPRO e está, atualmente, formalizada por meio do Acordo de Cooperação Técnica (ACT) nº 0731/2019, que estabelece as finalidades e resultados esperados da implementação e evolução dessa infraestrutura, além das obrigações dos parceiros. Resumidamente, à SGD/ME cabe a gestão da rede e dos serviços e ao SERPRO cabe a operação e manutenção da infraestrutura óptica e dos equipamentos da rede.

13.1.3 O serviço de Conexão Básica disponibiliza ao Demandante os seguintes atributos:

- Atendimento técnico 24 horas por dia e 7 dias por semana;
- Porta dedicada em switch de acesso;
- Segurança básica nível 2, por meio da separação do tráfego do cliente em VLANs (Virtual Local Area Network) privadas. A Segurança nível 2 está relacionada à camada 2 do Modelo OSI de redes, ou seja, segurança em nível de enlace. Em termos práticos, significa dizer que os tráfegos dos clientes participantes da rede Infovia Brasília não se misturam, são segmentados em estruturas de nível 2, ou seja, túneis virtuais configurados fim a fim;
- Disponibilidade mensal de 99,9%, exceto para conexões tipo 2;
- Latência de até 50ms, mensurada a partir do cliente até o Serpro Regional Brasília;
- Taxa de erro menor que 2%;
- Tratamento de falhas e interrupções com a geração e acompanhamento de indicadores de disponibilidade e apresentação de relatórios gerenciais de Indicadores no Portal do Cliente (<https://portaldocliente.serpro.gov.br>);

13.1.4 A modalidade de conexão Tipo 1

13.1.4.1 Modalidade de conexão utilizando 1 (um) *switch* com 2 (dois) pares de fibras de acesso redundantes ligados ao *backbone* da Infovia Brasília com bandas de 1(um) Gbps ou 10(dez) Gbps. Pode ser contratada em todas as localidades onde exista infraestrutura de rede da Infovia Brasília, mediante análise de viabilidade técnica pelas equipes do Serpro e SGD.

13.1.4.2 Neste tipo de conexão, o *switch* da Infovia Brasília poderá estar instalado em qualquer sala que tenha as condições técnicas necessárias para atendimento aos órgãos presentes na localidade. Ressalta-se que cada órgão ou entidade que possua conexão na mesma localidade será considerado como uma Conexão Tipo 1.

13.1.4.3 Detalhamento técnico da Conexão Tipo 1 – 10 Gbps: será disponibilizada uma porta física de 100/1000/10000 Mbps no *switch* de acesso com capacidade de tráfego de até 10 Gbps. Essa porta poderá ser UTP (até 10 Gbps) ou ótica – Monomodo ou Multimodo com conectorização LC (até 10Gbps).

13.1.5 Serviços Adicionais

13.1.5.1 Compreendem os serviços que podem ser adquiridos de forma adicional aos serviços de conexões básicas, pelo cliente ou órgão participante a fim de complementar a sua demanda, conforme sua necessidade.

13.1.6 Serviço de Acesso à Internet

13.1.6.1 Serviço de fornecimento de acesso à banda de Internet corporativa, sendo pré-requisito para a contratação deste, ser cliente Infovia Brasília (1Gbps), ou superior.

13.1.6.2 A largura de banda contratada é garantida ao cliente até a saída para os troncos públicos da Internet em que o Serpro está conectado. Atualmente, é composta por dois troncos de saída: Brasília e São Paulo, sendo cada um com três operadoras distintas, garantindo, redundância e resiliência da disponibilidade do serviço.

13.1.6.3 Nesse serviço, consta ainda o fornecimento de acesso à Internet na versão IPv6, em formato *dual stack*, conforme RFC 4241, compartilhando a mesma porta e banda onde ocorre o acesso à Internet na versão atual. São ofertados endereçamentos públicos em IPv4 e IPv6 conforme Tabela abaixo.

Faixa de Banda	Endereço IPv4	Endereço IPv6
1 Mbps a 100 Mbps	16	56
Acima de 100 Mbps	32	56

Tabela X - Quantidade de Endereços IP (IPv4 e IPv6) inclusos no serviço por faixa de velocidade contratada

13.1.6.4 O acesso à Internet se dá obrigatoriamente por meio de porta física dedicada de 100/1000/10000 Mbps (conforme tipo de conexão contratada). Entretanto, os recursos alocados para o provimento deste serviço não serão descontados da quantidade de portas previstas no pacote de Serviços Básicos.

13.1.6.5 Como melhoria dos aspectos de Segurança, todos os clientes que possuem o serviço de acesso à Internet Infovia Brasília, terão como serviço agregado AntiDDoS volumétrico. Esse tipo de ataque, pode esgotar o link do cliente e até mesmo tornar indisponíveis seus serviços *internet*. Com esse serviço, o cliente poderá informar até 6 (seis) endereços IP's que serão cadastrados na ferramenta do Serpro, para que seja feita a medição de tráfego dos IP's indicados e mitigação de possíveis ataques. Ao detectar uma anomalia na rede ou site específico dentro do bloco, o cliente deverá acionar o Serpro para que seja realizada a mitigação específica.

13.1.7 Fornecimento de Porta Adicional

13.1.7.1 Trata-se de configuração para utilização de 1 (uma) ou mais portas físicas adicionais no *switch* de acesso, além das portas já disponibilizadas para os serviços com previsão desse recurso. A porta da Conexão Básica não pode ser utilizada como porta adicional e nem eventual saldo de portas não utilizado em outra localidade.

13.1.7.2 A velocidade da porta será a mesma velocidade da conexão básica já contratada pelo cliente. Essas portas poderão ser UTP (até 1Gbps) ou óticas – Monomodo ou Multimodo com conectorização LC (até 10Gbps), dependendo da solicitação do cliente.

13.1.8 Serviços de Segurança

13.1.8.1 Segurança da Informação para Infovia: *Firewall*, Filtro de Conteúdo e IPS

13.1.8.2 O combo Segurança da Informação para Infovia possui uma solução única, contemplando três funcionalidades de proteção de forma agregada e indissociável. É uma alternativa que oferta recursos básicos de proteção, possibilitando um menor custo para o órgão ou entidade participante, mas sem deixar de lado a adequada proteção aos recursos informacionais, visando a proteção e controle do tráfego de rede desejado. O serviço é comercializado como uma solução única, fornecido exclusivamente para aqueles que utilizem o serviço Internet da Infovia. A solução é composta por 3 funcionalidades, descritas a seguir.

13.1.8.3 *Firewall*

13.1.8.4 Esta funcionalidade integra o serviço Segurança da Informação para Infovia e tem como função regulamentar a comunicação entre as redes de *internet*, *intranet*, Zonas Desmilitarizadas (ZDM), *extra-net's* e redes virtuais privadas (VPNs). Permite a proteção do perímetro, aplicações, servidores e infraestrutura de rede, provendo as características essenciais da segurança da informação, além de auditoria, autenticidade e privilégio mínimo. Essa regulamentação é feita baseada no princípio de privilégio mínimo, a partir da implementação e manipulação de uma base de regras, com instruções personalizadas e que reflitam a política de segurança de rede da organização. A funcionalidade consiste, em configurar e segmentar perfis de tráfego de rede em um ambiente dedicado ou compartilhado, mediante políticas de rede pré-definidas e estabelecidas em instâncias/contextos de *firewalls*, instalados em dispositivos físicos com grande capacidade de processamento e alta disponibilidade, disponível nos centros de dados do Serpro. A funcionalidade proporcionará um ambiente protegido por equipamentos especializados, configurados em alta disponibilidade e com alta capacidade de processamento. Será dedicada uma instância de *firewall* virtual com até 2.000.000,00 (dois milhões) de conexões simultâneas com capacidade de até 30 (trinta) Gbps de vazão de dados, sendo compartilhada por todos os clientes que utilizarem este serviço. Caso o cliente deseje um

ambiente totalmente exclusivo com maior capacidade, ele deverá escolher uma das demais modalidades disponíveis para o serviço de *Firewall*. Tais modalidades podem ser conhecidas na cartilha de comercialização do serviço de *Firewall*. Os equipamentos especializados, assim como as instâncias/contextos de *firewalls*, são monitorados, de forma a garantir a alta disponibilidade, com rápida intervenção para resolução de problemas em casos de falha. Mensalmente, são gerados relatórios com informações inerentes a disponibilidade. O serviço é monitorado pelo centro de comando. A monitoração da infraestrutura será realizada pelo Serpro, utilizando ferramentas específicas de monitoração, em regime de 24 horas durante 7 dias da semana. A funcionalidade provê a proteção em camadas dos serviços por meio de isolamento entre segmentos de rede – Separação dos ambientes, como exemplo os de produção, homologação e desenvolvimento, controle de acesso às aplicações de acordo com os perfis de acesso ao serviço.

13.1.8.5 A funcionalidade de *Firewall* dispõe de equipamentos físicos configurados em alta disponibilidade, com grande capacidade de processamento e alta densidade de interfaces de 1Gb e 10Gb. Além disso, dispõe de *software* especializado, capaz de virtualizar e dedicar recursos computacionais, assim como sistema operacional customizado de forma a garantir alta performance. Possui gerência centralizada, que garante a individualização de políticas de acesso para cada cliente. Ressalta-se no entanto que somente empregados do Serpro podem administrar os equipamentos.

13.1.8.6 Filtro de Conteúdo

13.1.8.7 Uma vez que o consumo de banda tornou-se um fator primordial, é necessário gerenciar esse consumo. Embora o acesso à *internet* seja uma fonte de benefícios inegáveis, pode também ser uma fonte para distração dos empregados de suas tarefas profissionais e permite, ainda, disponibilizar conteúdos inapropriados e/ou ofensivos, o que exige um controle por parte da empresa para o não desvirtuamento de sua utilização como ferramenta de trabalho. Para realização desse controle, o Serpro disponibiliza a funcionalidade de Filtragem de Conteúdo, cujo objetivo é monitorar e gerenciar o acesso às URL da *internet*. A Filtragem será feita através do desvio de tráfego *web*, oriundo da rede do cliente com destino à *internet*.

13.1.8.8 IPS

13.1.8.9 Tem como finalidade monitorar, detectar e bloquear ataques, direcionados aos serviços publicados pelo cliente da Infovia, provenientes da Internet ou da rede local, por meio de aplicação de assinaturas dedicadas. O monitoramento visa acompanhar o tráfego passante, comparando este com conhecidos padrões de ataque, mediante assinaturas definidas pelos fabricantes de equipamentos e outras criadas pelas equipes do Serpro, com o objetivo de bloquear tentativas de invasão que utilizem falhas em serviços publicados ou em estações de trabalho, como as conhecidas vulnerabilidades de *browser* e *intranet*. A funcionalidade de prevenção à Intrusão consiste na monitoração do tráfego através de equipamento ligado “in-line”, de forma que todo o tráfego que deve ser analisado passe por ele e seja inspecionado. O bloqueio aos ataques encontrados, a critério do cliente, podem ser apenas alertado ou bloqueado imediatamente, não permitindo desta forma a completa execução do ataque.

13.1.8.10 A funcionalidade é composta por: Sistema de Detecção de Intrusão; Assinaturas Atualizadas; Sistema de Proteção com Políticas Restritivas nas ZDMs e Sistema de ByPass Automático.

13.1.8.11 AntiDDoS - Proteção URL

13.1.8.12 O AntiDDoS Proteção URL é um serviço de proteção à sítios (site) contra ataques de negação de serviço distribuídos (DDoS), uso dos protocolos de acesso Internet de forma indevida e a otimização do uso da banda para publicação dos sítios.

13.1.8.13 Essa modalidade do serviço AntiDDoS possui maior quantidade de contra medidas para mitigação, por isso, é indicada para aplicações e/ou serviços de missão crítica ou afetem gravemente o negócio do cliente. Por ser mais específica que a proteção volumétrica, faz análise e detecção de anomalias com tempo de mitigação reduzido. Alguns outros recursos do serviço:

- Maior eficiência na mitigação de ataques de negação de serviços;
- Monitoramento 24x7;
- 5 horas de consultoria/Mês;
- Desenvolvimento de assinaturas personalizadas;
- *White and black list* específicas;
- Alteração dos arranjos de rede durante a ocorrência de ataques;
- Pacote completo de medidas preventivas (autenticação, Limite de taxa, escopo e malformação HTTP, expressão regular, autenticação DNS, DNS malformado, escopo DNS e limite de taxa DNS, etc).

13.2 Descrição geral do serviço de Rede de Longa Distância e *Backbone* SERPRO

13.2.1 A rede de longa distância, mundialmente conhecida como WAN (Wide Area Network), é formada pela interconexão dos pontos de acessos ao backbone do SERPRO associada à estrutura do próprio backbone e ao tronco internet e possibilita a transmissão de informações (voz, dados e imagem) com segurança e confiabilidade, mediante integração de várias tecnologias.

13.2.2 Essa rede está estruturada sobre tecnologia SDH (Synchronous Digital Hierarchy), que garante redundância física e tolerância a falhas. Além disso, é implementada logicamente como uma rede MPLS (Multiprotocol Label Switching), uma arquitetura voltada para a especialização e otimização de serviços.

13.2.3 A rede de dados do SERPRO utiliza a tecnologia de comutação de rótulos Multi Protocol Label Switching (MPLS) para estabelecer uma rede virtual privada VPN/IP. Essa solução combina inteligência de roteamento de alto desempenho, além de oferecer recursos de Qualidade de Serviço (QoS) e flexibilidade de operação em diferentes padrões de arquiteturas e serviços agregados. A rede é projetada para suportar elevado volume de tráfego de dados com segurança, alta resiliência e a máxima disponibilidade, adequado aos mais elevados níveis de serviço de aplicações críticas ou sistemas estruturantes, permitindo a conexão dos mesmos entre os diferentes pontos de um cliente contratante.

13.2.4 A infraestrutura central de comunicação (backbone) foi projetada para suportar o tráfego de grande volume de dados, com alto desempenho e máxima disponibilidade, para os mais variados tipos de serviço de tecnologia da informação (TI). Além disso, o *backbone* é estruturado com capacidade de redundância, que possibilita a alteração automática das rotas e mantém o tráfego ininterruptamente. Quando a rede de longa distância é complementada com o serviço de acesso à Internet, então camadas de segurança próprias da política de segurança do SERPRO também serão adicionadas à rede do DEMANDANTE, a exemplo do filtro de conteúdo web, prevenção de intrusão e proteção à ataques distribuídos de negação de serviço. Tais serviços são úteis para fazer uso do acesso à internet como meio de publicação, possibilitando a construção ZDMs dentro da rede do DEMANDANTE. Para isso o PROPONENTE fornece blocos de endereço IPv4 e IPv6. O gerenciamento integrado do serviço é executado conforme preceitua os modelos ISO e ITIL, adaptados às atividades do PROPONENTE. As informações de gerência são disponibilizadas através de um portal WEB, disponível 24 horas por 7 dias da semana, onde terá seu login e senhas exclusivos para acesso às informações de sua rede, através de relatórios, *dashboards* e mapas personalizados, conforme parâmetros de monitoração definidos. Tais parâmetros e escopo do gerenciamento podem ser formatados de acordo com as necessidades, mediante prévia avaliação de viabilidade técnica do PROPONENTE.

13.3 Descrição geral do serviço SERPRO Govshield

13.3.1 O GovShield oferece uma robusta proteção para sítios que vão desde ferramentas mais simples (como, por exemplo, aplicações, contratempo de inatividade e roubos de dados), bem como, para as mais avançadas (como, por exemplo, ataques DDoS), ambas com controles automatizados e integrados que responderão aos ataques muito rapidamente. Para tipos de ataques mais sofisticados que requerem uma resposta específica, será possível criar regras personalizadas. Essa plataforma de segurança em nuvem garante proteção no tráfego dos clientes com funcionalidades específicas, de acordo com as seguintes modalidades:

- Modalidade Bronze: possui funcionalidades suficientes para a proteção básica, onde o SERPRO faz toda a gestão e entrega os relatórios de segurança ao final do mês ou sob demanda;

- Modalidade Prata: possui funcionalidades básicas onde o SERPRO faz toda a gestão e o cliente só visualiza, com SLA da plataforma superior ao bronze e política de segurança personalizada; e

- Modalidade Ouro: possui funcionalidades em que a gestão é compartilhada entre SERPRO e cliente, com SLA da plataforma superior à prata e política de segurança personalizada.

13.3.2 Além das modalidades, o GovShield disponibiliza alguns adicionais conforme necessidade do cliente que são:

- Adicional de um 1 TB para Modalidade Bronze e Prata;
- Adicional de um 1 TB para Modalidade Ouro;
- Balanceamento de Carga;
- Zero Trust Network Access – Provisionamento inicial de até 50 usuários; e
- Zero Trust Network Access - Usuário extra.

13.3.3 Cada modalidade é vinculada a um domínio DNS e seus respectivos subdomínios pelo período de 1 (um) mês.

13.3.4 Caso o cliente possua mais de um domínio, haverá necessidade de contratação de outras modalidades (um domínio por modalidade).

13.3.5 Com o GovShield, o cliente se conecta aos seus aplicativos da Web por meio dos servidores de borda, que inspecionam o tráfego da Web para detectar e bloquear DDoS e ataques de aplicativos, enquanto acelera a entrega de conteúdo de seus aplicativos aos usuários. As modalidades bronze, prata e ouro possuem 1, 3 e 5 terabytes, respectivamente, disponíveis para proteção de sítios web no período de um mês.

13.3.6 Os adicionais de terabytes serão provisionados mensalmente somente se a aferição de tráfego limpo referente a modalidade exceder o limite contratado por três meses consecutivos, passando o montante de tráfego excedente do mês subsequente a ser aferido e pago como tráfego adicional.

13.3.7 Caso o consumo de *terabytes* retorne ao da modalidade contratada, reiniciará o ciclo de contagem de 3 (três) meses consecutivos, conforme item do parágrafo anterior.

14. Estimativa de custo total da contratação

Valor (R\$): 2.366.088,00

14.1. Conforme fundamentado no item 12.7, o valor total estimado para a contratação foi calculado com base nos valores da proposta do SERPRO, totalizando R\$ 2.192.856,00 (dois milhões, cento e noventa e dois mil, oitocentos e cinquenta e seis reais) para 12 meses. Este valor, que será efetivamente contratado, encontra-se dentro e abaixo do teto máximo orçamentário de R\$ 2.366.088,00 (**dois milhões, trezentos e sessenta e seis mil e oitenta e oito reais**) detalhado na Nota Técnica nº 4/Seinfra (SEI nº 09641843).

14.2. Ressalta-se que a solução é de natureza **escalável e modular**, o que implica que os itens não serão contratados de forma simultânea ou cumulativa, à exceção do **Item 1 (Conexão Tipo 1)**, que possui demanda fixa de 02 (duas) unidades mensais para a Funai-Sede e o Centro de Formação em Sobradinho.

14.3. Os demais itens de Conexão (Grupo A) e Segurança (Grupo B) operam em regime de **exclusividade mútua por patamar de tráfego**, sendo ativados sempre em pares correspondentes para garantir a integridade da solução (ex: Item 2 com Item 6; Item 3 com Item 7; Item 4 com Item 8).

14.4. A inclusão de todos os níveis de serviço na estimativa visa garantir a segurança jurídica e a flexibilidade necessária para que a Administração possa elevar ou reduzir a capacidade de tráfego e proteção conforme a necessidade sazonal, sem ultrapassar o limite orçamentário estabelecido.

A - SERVIÇO DE CONEXÃO - INFOVIA BRASÍLIA						
Item	Especificação	Unidade de Medida	Quantidade Contratada/Mês	Meses Estimados	Valor Unitário	Valor Estimado Total 12 MESES
1	INFOVIA - Conexão Tipo 1 a 10 Gbps	Mensal	2	12	R\$ 7.960,00	R\$ 191.040,00
2	INFOVIA - Serviço adicional de Conexão à Internet - Pacote de 400 Mbps	Mensal	1	12	R\$ 12.000,00	R\$ 144.000,00
3	INFOVIA - Serviço adicional de Conexão à Internet - Pacote de 700 Mbps	Mensal	1	12	R\$ 15.400,00	R\$ 184.800,00
4	INFOVIA - Serviço adicional de Conexão à Internet - Pacote de 1Gbps	Mensal	1	12	R\$ 16.000,00	R\$ 192.000,00
5	INFOVIA - Adicional Internet – Excedente 1000 Mbps	mbps	500	12	R\$ 16,00	R\$ 96.000,00
Valor estimado dos serviços continuados, referentes aos Itens 1 a 5						R\$ 807.840,00
B - SERVIÇO DE SEGURANÇA						
Item	Especificação	Unidade de Medida	Quantidade Contratada/Mês	Meses Estimados	Valor Unitário	Valor Estimado Total 12 MESES
6	INFOVIA – Adicional Segurança – Pacote 400 Mbps	Mensal	1	12	R\$ 24.096,00	R\$ 462.384,00
7	INFOVIA – Adicional Segurança – Pacote 700 Mbps	Mensal	1	12	R\$ 33.382,00	R\$ 400.584,00
8	INFOVIA – Adicional Segurança – Pacote 1 Gbps	Mensal	1	12	R\$ 38.625,00	R\$ 463.500,00
9	INFOVIA – Adicional Segurança – Excedente 1 Gbps	mbps	500	12	R\$ 38,63	R\$ 231.780,00
Valor estimado dos serviços continuados, referentes aos Itens 6 a 9						R\$ 1.558.248,00
Valor estimado da contratação para 12 meses (A+B)		R\$ 2.366.088,00				

Tabela XI - Consolidação dos valores referenciais de mercado para a solução escalável

15. Justificativa técnica da escolha da solução

15.1 Em consideração ao exposto nos itens 10 e 11 deste ETP, a escolha da contratação dos serviços pelo SERPRO representa expertise e especialização por se tratar de uma empresa pública onde os projetos são executados de formas mais eficiente e com menor risco de falhas e retrabalhos. Ao contratar com o SERPRO, a Administração Pública acessa um conhecimento técnico aprofundado, que seria caro e demorado para construir internamente ou para ser contratado de uma empresa privada que não tem o mesmo nível de especialização no contexto governamental.

15.1.1 O Serpro atende a centenas de órgãos e entidades públicas, o que permite um ganho de escala significativo. A infraestrutura de *data centers*, redes (como a **Infovia**) e plataformas de segurança (como o **GovShield**) é compartilhada por diversos clientes. Isso dilui os custos de investimento, manutenção e operação, tornando cada serviço individual mais barato para cada órgão. Em vez de cada ministério construir sua própria infraestrutura do zero, eles se beneficiam de uma solução já existente e robusta. A Administração Pública garante que suas informações estejam em um ambiente seguro, sob jurisdição nacional e com governança alinhada aos interesses do Estado. A proteção contra ataques cibernéticos, fraudes e vazamentos de dados é um custo de segurança que, se fosse gerido individualmente por cada órgão, geraria despesas altíssimas. O Serpro oferece esse serviço de forma centralizada, com monitoramento 24 /7 e uma equipe especializada, resultando em uma proteção mais eficaz e econômica.

15.1.2 Importa registrar que a contratação de serviços junto ao SERPRO gera economicidade que não se resume ao preço de tabela, mas ao valor agregado em termos de segurança, confiabilidade, sinergia entre os órgãos públicos e redução de custos de implantação e manutenção a longo prazo, em consonância com o disposto no inciso IX do art. 75 da Lei nº 14.133, de 1º de abril de 2021, que autoriza a contratação direta de empresa pública criada para a execução de serviços de natureza compatível com o seu objeto social. Trata-se de um modelo que maximiza o retorno sobre o investimento público em tecnologia.

15.1.3 Da Conformidade com a Portaria SGD/MGI nº 5.950/2023:

Esta equipe de planejamento declara que a solução de segurança em nuvem (Firewall/WAF - GovShield) foi modelada em estrita observância à Portaria SGD/MGI nº 5.950/2023. O enquadramento fundamenta-se no Art. 2º, inciso IV, por tratar-se de serviço de computação em nuvem. A opção pelo modelo de provimento via empresa pública federal (SERPRO) é justificada tecnicamente pela necessidade de integração nativa e isolamento lógico (Camada 2) com a rede INFOVIA Brasília, requisito de segurança essencial para a proteção do tráfego governamental que não é plenamente atendido pelos modelos de nuvem pública genérica. Ressalte-se que a solução é transitória e necessária até que a FUNAI implemente sua solução própria de firewall, garantindo a continuidade da proteção conforme o Anexo I da referida Portaria.

15.2 Ao analisar as soluções ofertadas pelo Serpro em conjunto, constata-se a representação de um ecossistema de infraestrutura e segurança. Ao contratá-las, o governo garante uma base sólida para a transformação digital. Destaca-se também a vantagem da contratação com empresa pública para mitigar o risco de não continuidade do negócio e a promoção de utilização de níveis de serviço e metas mais alinhadas com a área de negócio institucional, conforme os benefícios listados no item 18 deste Estudo Técnico. Segurança e soberania digital.

16. Justificativa econômica da escolha da solução

16.1 Como demonstrado nos itens 10 e 11 deste documento, a solução escolhida é a contratação do Serviço Federal de Processamento de Dados - Serpro - para prestação dos serviços de Infovia e serviço de segurança GovShield com fulcro no art. 75, IX, da lei n. 14.133 /2021 - Dispensa de Licitação.

16.2 Em que pese se tratar de uma contratação direta, foi realizada análise/comparativo de preços, demonstrado na Nota Técnica 4 (09641843) a qual evidencia que não há discrepâncias ou sobrepreço, entre os valores praticados/ofertados a este Instituto (SEI 09642652) e contratações com objetos similares prestados pelo Serpro. Ref: Art. 5º, II e Art. 7º, § 4º da Instrução Normativa Seges /Me nº 65, de 7 de Julho de 2021.

17. Parcelamento da Solução

17.1 Objetiva-se realizar uma contratação única com o mesmo fornecedor, Serpro, considerando os benefícios agregados aos serviços que serão contratados, principalmente, em relação à segurança de dados e cibernética, sob a ótica da eficiência e da economicidade, uma vez que gerará economia de escala e redução de custos.

17.2 Outro ponto a ser considerado na contratação com o único fornecedor é a simplificação do processo de gestão e fiscalização. Para a administração gerenciar vários contratos com diferentes fornecedores, prazos, aditivos e obrigações, gera custo e tempo, assim uma

contratação única tem o papel de simplificar o trabalho da equipe responsável, desde o acompanhamento da entrega dos itens até a fiscalização da qualidade do serviço prestado gerando menos burocracia e trazendo maior agilidade e menor risco de erros administrativos para os gestores envolvidos.

17.3 E, ainda, busca-se com uma contratação única a garantia maior de que os produtos e os serviços terão características e padrões de qualidade semelhantes e compatibilidade para tornar o ambiente computacional do Funai seguro e otimizado nas prestações dos serviços de TIC.

17.4 Em vista disso, para a presente contratação, o parcelamento não será adotado, conforme aderência ao disposto no §3º do art. 40 da Lei 14.133 de 2021:

[...]

Art. 40. O planejamento de compras deverá considerar a expectativa de consumo anual e observar o seguinte:

[...]

§ 3º O parcelamento não será adotado quando:

I - a economia de escala, a redução de custos de gestão de contratos ou a maior vantagem na contratação recomendar a compra do item do mesmo fornecedor;

II - o objeto a ser contratado configurar sistema único e integrado e houver a possibilidade de risco ao conjunto do objeto pretendido;

III - o processo de padronização ou de escolha de marca levar a fornecedor exclusivo.

[...]

18. Benefícios a serem alcançados com a contratação

18.1 Benefícios para o órgão

18.1.1 Redução de gastos, em função do maior controle das compras governamentais nas áreas de telecomunicações e da possibilidade de maior economia na contratação conjunta de serviços, como telefonia fixa e *Internet*, uma vez que é possível utilizar a infraestrutura da Infovia Brasília para distribuir os serviços entre os órgãos públicos;

18.1.2 Contribuir com a padronização de soluções de comunicação e de conectividade dos órgãos da APF;

18.1.3 Maior flexibilidade em expansões futuras e em adoção de novas aplicações de serviços demandantes de maior banda de comunicação;

18.1.4 Garantia de um padrão elevado de qualidade de serviço nas comunicações entre órgãos e com a Internet, bem como da qualidade dos serviços de telecomunicações prestados aos órgãos da APF;

18.1.5 Aumento do sigilo e da segurança da informação, relacionados às comunicações do governo federal e nas trocas de informações e documentos entre os órgãos públicos;

18.1.6 Melhor desempenho dos serviços e aplicações que utilizam redes de comunicações de dados de alta taxa de transmissão;

18.1.7 Preservação da propriedade sobre a infraestrutura da rede pelo governo, possibilitando maior flexibilidade nas decisões de adoção de novos serviços e com maiores capacidades para APF;

18.1.8 Maior independência em relação às empresas privadas prestadoras de serviço de rede e de telecomunicações;

18.1.9 Aumento da confiabilidade das informações governamentais que trafegam nas redes;

18.1.10 Aumento da agilidade no atendimento às demandas dos cidadãos.

18.1.11 Suprir os serviços de TIC com soluções que buscam atender ao mercado público, direto ou indireto, nas esferas municipal, estadual e federal;

18.1.12 Soluções de fácil gerenciamento;

18.1.13 Monitoramento e atuação do ambiente em tempo real;

18.1.14 A **Infovia** é uma rede de comunicação exclusiva para órgãos e entidades públicas. Contratar essa solução traz vantagens fundamentais para a infraestrutura de TI:

- **Segurança aprimorada:** Por ser uma rede dedicada, a Infovia oferece um nível de segurança muito maior do que a internet pública, com funcionalidades como firewall, filtro de conteúdo e proteção contra ataques de negação de serviço (DDoS).
- **Alta velocidade e capacidade:** A Infovia garante uma infraestrutura robusta com alta capacidade de tráfego (podendo chegar a 10 Gbps), o que é essencial para sistemas que lidam com grandes volumes de dados.
- **Redundância e disponibilidade:** A estrutura da Infovia conta com redundância física e lógica, garantindo que o serviço continue funcionando mesmo em caso de falhas, com alta taxa de disponibilidade.
- **Economia e eficiência:** Ao oferecer uma solução única e agregada, a Infovia evita que os órgãos precisem contratar diversos serviços de conectividade separadamente, o que resulta em redução de custos e maior eficiência na gestão.

19. Providências a serem Adotadas

19.1 Não serão necessárias adequações no ambiente da Funai ou capacitação para a gestão e fiscalização do Contrato Administrativos pelos servidores que serão incumbidos dessa atividade.

20. Declaração de Viabilidade

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

20.1. Justificativa da Viabilidade

A contratação proposta mostrase viável sob os aspectos técnicos, operacionais e administrativos apresentados ao longo deste Estudo. As análises realizadas nos itens anteriores demonstram que a solução atende aos requisitos de conectividade, segurança, disponibilidade e integração necessários ao funcionamento dos sistemas e das atividades finalísticas da Funai. Além disso, os cenários avaliados evidenciaram que as alternativas existentes no mercado não oferecem, de forma simultânea, os elementos essenciais para manter a continuidade da operação, o isolamento adequado do tráfego e a compatibilidade com a infraestrutura já implantada.

Os custos estimados encontram-se alinhados às referências de mercado e foram validados por meio de pesquisa de preços, garantindo aderência às normas de planejamento e de eficiência do gasto público. A solução apresenta ainda caráter escalável, permitindo adequação gradual conforme a necessidade, o que contribui para sua viabilidade econômica e operacional. Assim, reunidos os elementos técnicos, econômicos e institucionais apresentados, conclui-se que a contratação é viável e atende ao interesse público, assegurando a continuidade dos serviços e o suporte necessário às atividades da Funai.

Justificativa para a Não Exigência de Garantia Contratual: A equipe de planejamento opta por não exigir a prestação de garantia de execução (Art. 96 da Lei nº 14.133/2021) para esta contratação. Tal decisão fundamenta-se no fato de a futura contratada ser o **SERPRO**, empresa pública federal vinculada ao Ministério da Fazenda, o que confere elevada solvência e reduz o risco de descontinuidade empresarial ou inadimplemento contratual por insolvência. Além disso, o objeto (Infovia e Segurança) é um serviço continuado com medição e pagamento mensais após o ateste, permitindo à Administração realizar glosas e retenções preventivas em caso de falhas na prestação, o que torna a exigência de caução ou seguro-garantia um ônus administrativo e financeiro desnecessário.

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](#).

EDUARDO ALMEIDA SANTOS OLIVEIRA

Integrante Técnico



Assinou eletronicamente em 14/04/2026 às 14:48:09.

BRUNO ALVES DE LIMA

Integrante Requisitante



Assinou eletronicamente em 13/04/2026 às 18:46:48.

TIAGO OLIVEIRA LOUP

Autoridade Máxima de TIC



Assinou eletronicamente em 14/04/2026 às 14:25:03.