



INSTITUTO NACIONAL DE COLONIZAÇÃO E REFORMA AGRÁRIA
ESTUDO TÉCNICO PRELIMINAR DA CONTRATAÇÃO - TI

Processo nº 54000.056994/2021-81

INSTITUTO NACIONAL DE COLONIZAÇÃO E REFORMA AGRÁRIA - INCRA
ESTUDO TÉCNICO PRELIMINAR DA CONTRATAÇÃO (ETPC)

CONTRATAÇÃO DE SERVIÇOS TÉCNICOS ESPECIALIZADOS PARA CONECTIVIDADE, SD-WAN E ESTAÇÃO DE TRABALHO VIRTUAL

Processo nº 54.000.056994/2021-81.

1. INTRODUÇÃO (IN SGD/ME Nº 01/2019, ARTS 1º, 2º, 9º)

1.1. Em observância ao que está previsto na Instrução Normativa nº 01, de 04 de abril de 2019 e na Instrução Normativa nº 31, de 23 de março de 2021 foi desenvolvido este Estudo Técnico Preliminar da Contratação (ETPC) tem por objetivo identificar e analisar os cenários para o atendimento **Solução de Serviços técnicos especializados para Conectividade (Links de Internet), SD-WAN e Estação de trabalho virtual (VDI)** com foco em mobilidade, conexão de internet e centralização de acesso, contemplando empresa especializada na operação, suporte e repasse de conhecimento, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação.

1.2. Nesse contexto, o **objeto desta contratação é uma solução de Tecnologia da Informação e Comunicação (TIC)**, pois apoia os processos de negócio, mediante a prestação de serviços técnicos especializados para o fornecimento de links de internet com velocidade compatível com o mercado, mas que garanta conectividade de alta performance 24 horas por 7 dias da semana (24x7) para Sede, Superintendências (SR's) e Unidades Avançadas (UA's) com ou sem redundância; de solução de espaço de trabalho virtual ou infraestrutura de desktop virtual, comumente conhecido como VDI (Virtual Desktop Infrastructure); e de serviço para aquisição de solução de aceleração/otimização de tráfego WAN, implementação e configuração de rede definida por software (SD-WAN). Dessa maneira, se enquadra no conceito de solução de TIC da IN SGD/ME 01/2019, Artigo 2, Inciso VII:

"solução de TIC: conjunto de bens e/ou serviços que apoiam processos de negócio, mediante a conjugação de recursos, processos e técnicas utilizados para obter, processar, armazenar, disseminar e fazer uso de informações;" (GRIFO NOSSO)

1.3. Sendo o INCRA uma entidade integrante do SISP, esta contratação de TIC deve ser disciplinada pela IN SGD/ME 01/2019 conforme caput do seu artigo 1º:

"As contratações 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 serão disciplinadas por esta Instrução Normativa." (GRIFO NOSSO)

1.4. Conforme inciso XI do artigo 2º da IN SGD/ME 01/2019, o Estudo Técnico Preliminar (ETPC) é o documento que descreve as análises realizadas em relação às condições da contratação em termos de necessidades, requisitos, alternativas, escolhas, resultados pretendidos e demais características, e que demonstra a viabilidade técnica e econômica da contratação.

1.5. Observa-se, ainda, que o Artigo 9º da IN SGD/ME 01/2019, a elaboração do ETPC é obrigatória e é a segunda etapa do planejamento da contratação.

1.6. Ressalta-se que este ETPC é resultado de um processo interativo, incremental e que recebeu contribuições técnicas a partir da análise de mercado e de preços da solução que se pretende adquirir. Logo, acredita-se que este estudo esteja em consonância com as necessidades negociais do Incra e compatível com as Boas Práticas de mercado para minimizar os riscos no processo de licitação quanto a aderência de requisitos técnicos, pois também objetiva demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação e acredita-se que a solução unificada para atender todas as unidades organizacionais trará benefícios significativos para o INCRA, principalmente ao observar as recomendações do órgão de controle para que se tenham uma área TI unificada para se evitar TIs paralelas.

1.7. Ademais, esta pretensa contratação faz parte dos processo de investimentos em Segurança da Informação e Comunicações (SIC), haja vista que será contemplado serviços especializados voltados para esse tema que se tornaram uma tendência nos mais diversos órgãos após os recentes incidentes de segurança cibernética que está assolando várias instituições públicas e privadas, inclusive o Departamento de Segurança da informação - DSI, divulgou Alerta Especial nº 07/2020 a respeito de campanhas de ataques de *ransomware*, conforme Documento SEI Relatório Recomendações CTIR-GOV (SEI nº 7691929).

1.8. Deve-se considerar, também, que a pretensa contratação está prevista no Plano Diretor de Tecnologia da Informação e Comunicação do Incra previsto para o período de Ago/2021 a Ago/2024 (Plano Diretor de TIC 2021-2024 | SEI nº 9793479) em sua página 58 como Necessidade de Contratação de números 029, 045 e 052 e para substituir o Contrato 43.200/2017, cujo objeto é a prestação de serviços especializado de Telecomunicação, por meio de Redes IP, utilizando tecnologia MPLS, haja vista que esse contrato não atende todas as unidades organizacionais e por apresentar limitações para expansão e outros fatores que serão demonstrados neste documento.

1.9. A Secretaria de Gestão do Ministério da Economia lançou o Sistema ETP Digital, que, conforme Instrução Normativa Seges/ME nº 40, de 22 de maio de 2020, passou a ser obrigatório desde 1º de julho de 2020 para as aquisição de bens e a contratação de serviços e obras federais, **exceto para as soluções de Tecnologia da Informação e Comunicações (TIC)**.

1.10. O documento referência ao item anterior, consta no sítio <https://www.gov.br/compras/pt-br/images/Orientao-da-SGD-quanto-ao-Sistema-ETP-Digital.pdf> (Orientação da SGD quanto ao ETP Digital para contratações de TIC).

2. DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITOS (IN SGD/ME Nº 01/2019, ART.11, INCISO I) NÃO MODIFICADO PELA IN Nº 31/2021

2.1. Identificação das necessidades de negócio

- 2.1.1. Corroborar com a transformação digital no INCRA;
- 2.1.2. Centralizar os sistemas e bases de dados sob a gestão do INCRA Sede;
- 2.1.3. Criar transparência sobre as atividades dos servidores/colaboradores do INCRA;
- 2.1.4. Implementar portal de trabalho virtual seguro para os servidores/colaboradores;
- 2.1.5. Inibir o vazamento de dados e informações sigilosas;

- 2.1.6. Minimizar o impacto de riscos ao negócio;
 - 2.1.7. Entregar níveis resilientes de serviços aos servidores/colaboradores;
 - 2.1.8. Melhorar a entrega de aplicações e dados para superintendências regionais e unidades avançadas;
 - 2.1.9. Melhorar a segurança da informação e comunicação no INCRA;
 - 2.1.10. Manter infraestrutura adequada às necessidades do Incra e aos novos padrões e tecnologia e normatizações como LGPD;
 - 2.1.11. Atender aos requisitos de disponibilidade dos serviços e soluções de tecnologia da informação disponibilizadas pelo INCRA ao seu público interno e à sociedade;
 - 2.1.12. Aderir ao modelo de teletrabalho maturado durante a pandemia e amplamente utilizado no poder público;
 - 2.1.13. Permitir aos colaboradores o suporte ao BYOD (*Bring Your on Device* - Traga seu próprio dispositivo) para uso no trabalho diário, com incremento de segurança e controle dos dados, independentemente da plataforma utilizada;
 - 2.1.14. Conectar os usuários das unidades remotas às aplicações e dados centralizados por meio de conexão de rede veloz e altamente disponível.
 - 2.1.15. Minimizar os riscos de indisponibilidade e outros relacionados à segurança cibernética;
 - 2.1.16. Atualizar a forma de acesso remoto e teletrabalho dos servidores/colaboradores.
- 2.2. **Identificação das necessidades tecnológicas**
- 2.2.1. Facilitar suporte aos colaboradores do INCRA e suas unidades remotas com capacidade avançada de investigação;
 - 2.2.2. Coletar e inspecionar informações de eventos em tempo real para auxiliar no suporte aos usuários, uma vez que todos os conteúdos estão virtualizados e em posse do INCRA, pode-se realizar um suporte muito mais ágil;
 - 2.2.3. Aumentar a disponibilidade e segurança de dados e aplicações críticas do INCRA;
 - 2.2.4. Possibilidade de entrega performática de aplicações legadas e com antigos requisitos tecnológicos;
 - 2.2.5. Permitir acesso seguro às aplicações e dados mesmo que o usuário utilize uma máquina desatualizada e passível de vulnerabilidades sem comprometer a organização;
 - 2.2.6. Melhorar a conectividade das unidades remotas com o INCRA Sede através de conexão de link redundante e com balanceamento automático;
 - 2.2.7. Monitorar a qualidade de uso dos links atendendo sempre pelo link melhor disponível e utilização simultânea dos links a fim de garantir o investimento;
 - 2.2.8. Aumentar a disponibilidade e garantir a entrega de aplicações institucionais legadas como o SIGEF, SIPRA, SNCCI, SEI, etc., independente do dispositivo utilizado para o acesso;
 - 2.2.9. Centralizar dados para permitir a utilização destes de uma forma mais inteligente e segura;
 - 2.2.10. Realizar configuração de segurança para acesso contextual e por usuários ou grupos, com políticas granulares atendendo aos diversos modelos de negócio, sem a necessidade de softwares extra nas máquinas dos colaboradores;
 - 2.2.11. Permitir que usuários das superintendências regionais e unidades avançadas possam utilizar uma infraestrutura ágil, segura e disponível para acesso aos recursos virtualizados de forma centralizadas, obtendo-se maior segurança e alto nível de gerência.
- 2.3. **Demais requisitos necessários e suficientes à escolha da solução de TIC**
- 2.3.1. Melhorar a continuidade e disponibilidade dos serviços de TIC;
 - 2.3.2. Realizar atualização tecnológica;
 - 2.3.3. Otimizar o uso dos recursos computacionais;
 - 2.3.4. Reduzir os incidentes e indisponibilidades para os colaboradores;
 - 2.3.5. Funcionalidades tecnológicas como experiência unificada, gestão de políticas de dados, controle de acesso e análise em tempo real de usuários, para que estejam preparadas para a nova forma de trabalho digital;
 - 2.3.6. Prover de confidencialidade, integridade e disponibilidade das informações.
3. **IDENTIFICAÇÃO DO AMBIENTE ATUAL (IN SGD/ME Nº 01/2019, ART.11, INCISO I)**
- 3.1. **Atual cenário de conectividades entre INCRA Sede e unidades remotas**
- 3.1.1. Instituto Nacional de Colonização e Reforma Agrária (INCRA) é uma Autarquia Federal vinculada ao Ministério da Casa Civil, criada pelo Decreto-Lei nº 1.110, de 9 de julho de 1970. Atualmente, o INCRA possui estrutura organizacional diretiva composta pelas seguintes unidades: Gabinete da Presidência (GAB), Diretoria de Gestão Estratégica (DE), Diretoria de Gestão Operacional (DO), Diretoria de Governança Fundiária (DF), Diretoria de Desenvolvimento e Consolidação de Projetos de Assentamento (DD).
- 3.1.2. Além de suas Diretorias, o INCRA possui em sua organização **78 unidades**, sendo 01 Sede, 29 Superintendências Regionais (SR), 02 Unidades Avançadas Especiais (UAE) e 46 Unidades Avançadas (UA), as quais são responsáveis por executar a Política Nacional de Reforma Agrária (PNRA) a cargo do INCRA. Atualmente, o INCRA comporta políticas voltadas ao Acesso à Terra, Crédito, Infraestrutura, Educação, Meio Ambiente, Geração de Renda e Ordenamento e Estrutura Fundiária. Toda a UA está administrativamente vinculada à uma SR, e essas SR's vinculadas à Sede.
- 3.1.3. Por ser uma organização complexa e com políticas desafiadoras, existe uma grande necessidade de mapeamento, integração, comunicação e confiabilidade nos seus processos de negócio e fluxos de trabalho. Neste documento, serão citados como unidades remotas, as Superintendências Regionais (SR's) e as Unidades Avançadas (UA's). No decorrer desse documento, por vezes as duas Unidades Avançadas Especiais (UAE) serão suprimidas, apresentando-se apenas como UA, já que possuem estrutura igual ou semelhante as UA's.
- 3.1.4. O INCRA Sede é a entidade responsável por prover infraestrutura e soluções tecnológicas adequadas à essas entidades subsidiárias (SR's e UA's). As unidades remotas SR's possuem conexão de rede do tipo MPLS (*Multi Protocol Label Switching*), que é uma comunicação corporativa entre essas unidades e a Sede. As UA's não possuem esse tipo de conectividade baseada em MPLS, utilizando, geralmente, conexão de Internet comum. Entretanto em algumas unidades menores e remotas, por vezes foi possível identificar usuários utilizando conexão de Internet pessoal de seu smartphone (3G ou 4G) devido a problemática atual de conectividade. Além disso, não tem sido incomum constantes comunicados de problemas relacionados a internet e na maioria dos casos está relacionado a banda disponível, por exemplo o Processo SEI 54000.086057/2021-50 relacionado a SR(27) Marabá que elaborou o Relatório (SEI nº 9949147): *in verbis*

"a) **URGENTE** – Atendimento ao pleito constante nos autos 54000.060215/2021-41, no qual fora relatada a **deficiência no serviço de Internet que tem impossibilitado até mesmo a execução de serviços simples como a assinatura de documentos no SEI, impactando negativa e significativamente na titulação.**

A inoperância dos sistemas em decorrência do acesso deficitário à internet é tão sério que este subscritor e os demais servidores da Regional estão se vendo obrigados a 7 usarem a internet de seus celulares ou permanecerem despachando no horário de almoço e até mesmo após as 19h para obter algum resultado." (GRIFO NOSSO)

3.1.5. O fornecimento atual é pelo protocolo MPLS que consiste em uma tecnologia de chaveamento de pacotes que possibilita o encaminhamento e a comutação eficientes de fluxos de tráfego através da rede, apresentando-se como uma solução para diminuir o processamento nos equipamentos de rede e interligar com maior eficiência redes de tecnologias distintas. O INCRA utiliza tecnologia do tipo MPLS para conectar as unidades remotas SR's com a Sede, a fim de prover os recursos de tecnologia necessários para essas unidades. Essa conexão não utiliza de link público ou de internet, sendo essa comunicação trafegada em conexão dedicado ao INCRA e suas unidades remotas, com isso essa comunicação cria uma rede privada entre essas localidades. O INCRA possui um contrato ativo com a operadora CLARO/EMBRATEL (**Contrato nº 43.200/2017 0115397, Pag. 206**) para entrega de conexão MPLS dedicada, interligando as unidades remotas do INCRA à sua Sede.

3.1.6. Ademais, é mister mencionar os aspectos relacionados ao Programa de Gestão da Continuidade de Negócios - PGCN, em especial quanto a garantir a continuidade de fornecimento de produtos e serviços com base na IN06/IN01/DSIC/GSIPR e apontamentos do Acórdão TCU 1603/2008 para manter a continuidade da prestação do serviço público pelo Incra:

"Programa de Gestão da Continuidade de Negócios é um processo contínuo de gestão e governança suportado pela alta direção e que recebe recursos apropriados para garantir que os passos necessários estão sendo tomados de forma a identificar o impacto de perdas em potencial, manter estratégias e planos de recuperação viáveis e garantir a continuidade de fornecimento de produtos e serviços por intermédio análises críticas, testes, treinamentos e manutenção." IN06/IN01/DSIC/GSIPR (GRIFO NOSSO)

"9.1.3 orientem sobre a importância do gerenciamento da segurança da informação, promovendo, inclusive mediante normatização, ações que visem estabelecer e/ou aperfeiçoar a gestão da continuidade do negócio, a gestão de mudança, a gestão de capacidade, a classificação da informação, a gerencia de incidentes, a análise de riscos de TI, a área específica para gerenciamento da segurança da informação, a política de segurança da informação e os procedimentos de controle de acesso" Acórdão TCU 1603/2008 (GRIFO NOSSO)

3.1.7. Essa comunicação estende os recursos de aplicações e dados para as SR's, deste modo, uma SR nativamente pode se conectar na Sede sem nenhuma intervenção por parte do usuário, porém com conexão sem redundância ou alta disponibilidade, uma vez que as SR's possuem apenas um link MPLS disponível. Já uma UA quando necessita de acesso às aplicações disponibilizadas pelo INCRA, utiliza conectividade de Rede Privada Virtual (Virtual Private Network - VPN) com o Datacenter Sede, sendo assim, uma UA sempre se conectará ao INCRA Sede através de sua conexão via VPN para consumir recursos tecnológicos. Uma conexão VPN (Virtual Private Network) estabelece uma conexão criptografada, chamada de "conexão segura", entre o usuário e o INCRA. Esta conexão é nomeada conexão VPN client-to-site, pois neste caso, é uma conexão iniciada pelo cliente afim de conectar no site remoto, neste caso, o datacenter do INCRA Sede. Por meio da VPN, todo o tráfego de dados é roteado por um túnel virtual criptografado. A conexão por meio de um Cliente VPN, torna o usuário da unidade remota UA, capaz de acessar recursos computacionais dentro do datacenter do INCRA Sede.

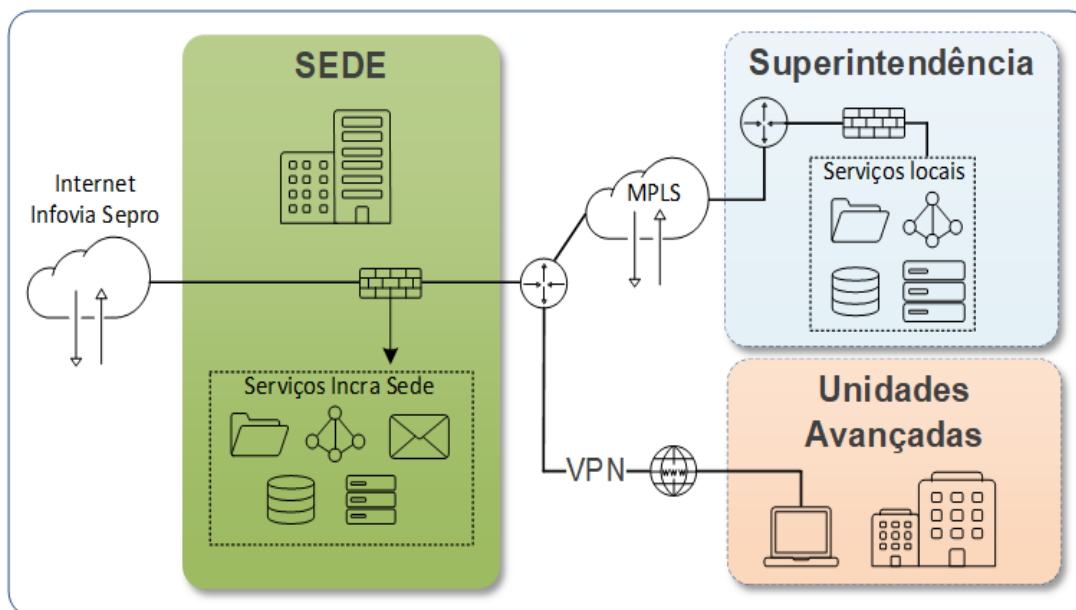


Figura 1: Conexão de unidades remotas à Sede.

3.1.8. Esse modelo onde não há uma uniformidade de acesso por parte das unidades remotas para acessar os recursos da Sede, dificulta a gestão e distribuição de aplicações por parte o INCRA Sede. As unidades avançadas utilizam conexão de internet comum e única para se conectar à Sede, e as superintendências regionais utilizam também link único de tecnologia MPLS, sendo assim, em ambas as unidades remotas há um fator de falha e falta de segurança, uma vez que não há componentes de tecnologia que garantam a idoneidade do acesso por parte dos colaboradores até o INCRA Sede ou até a Internet, sendo uma falta crítica de controle e gestão de acesso aos dados e aplicações. A malha de conexão de rede MPLS atualmente implementada, possui um custo elevado de contrato, além das já citadas fragilidades.

3.1.9. Quando os servidores/colaboradores se encontram executando seu trabalho presencialmente em alguma SR, esses servidores/colaboradores eventualmente utilizam tanto as aplicações locais não homologadas, localizadas na SR's, quanto as aplicações corporativas providas pelo INCRA Sede, utilizando a conexão de rede baseada na malha MPLS. Esses servidores/colaboradores utilizam seus recursos computacionais como se (logicamente) estivessem dentro das dependências do INCRA Sede, porém sendo por vezes impactados pela fragilidade de conexão única e na não redundante entre a Sede e as unidades remotas.

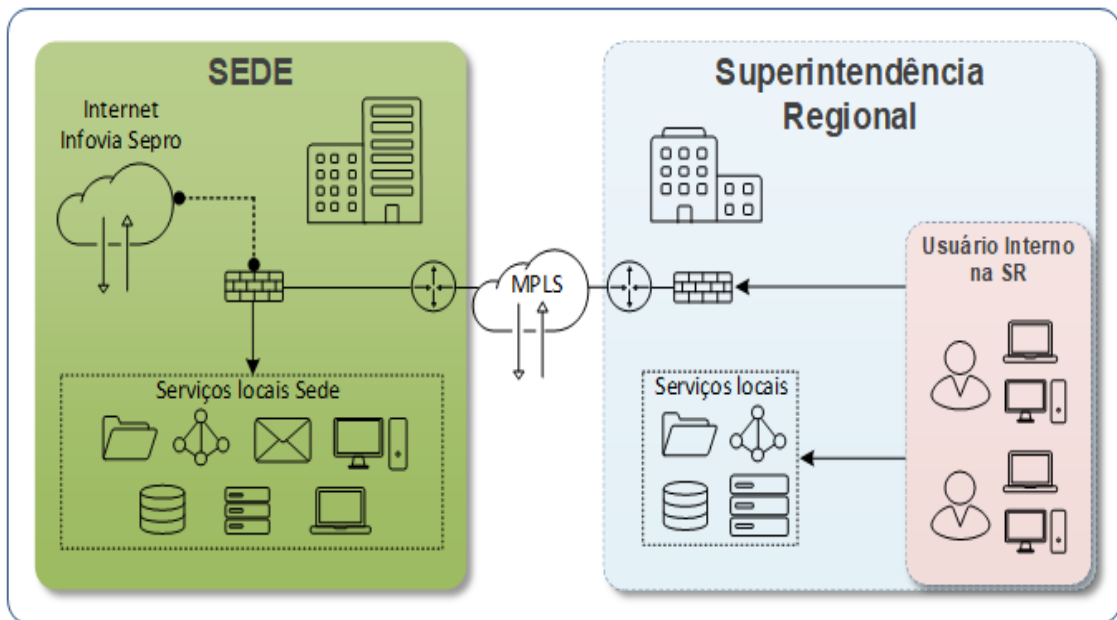


Figura 2: Conexão de usuários internos (colaboradores das SR's).

3.1.10. A rede MPLS utiliza de uma conexão antiga, essas redes são amplamente usadas para as aplicações empresariais, no entanto, deixam a desejar quanto à qualidade do serviço. A rede atual, implementa uma rede privada estendida entre as localidades remotas do INCRA e a Sede, sendo com isso, necessário que todos os acessos à Internet sejam direcionados à Sede e essa por sua vez provê este acesso.

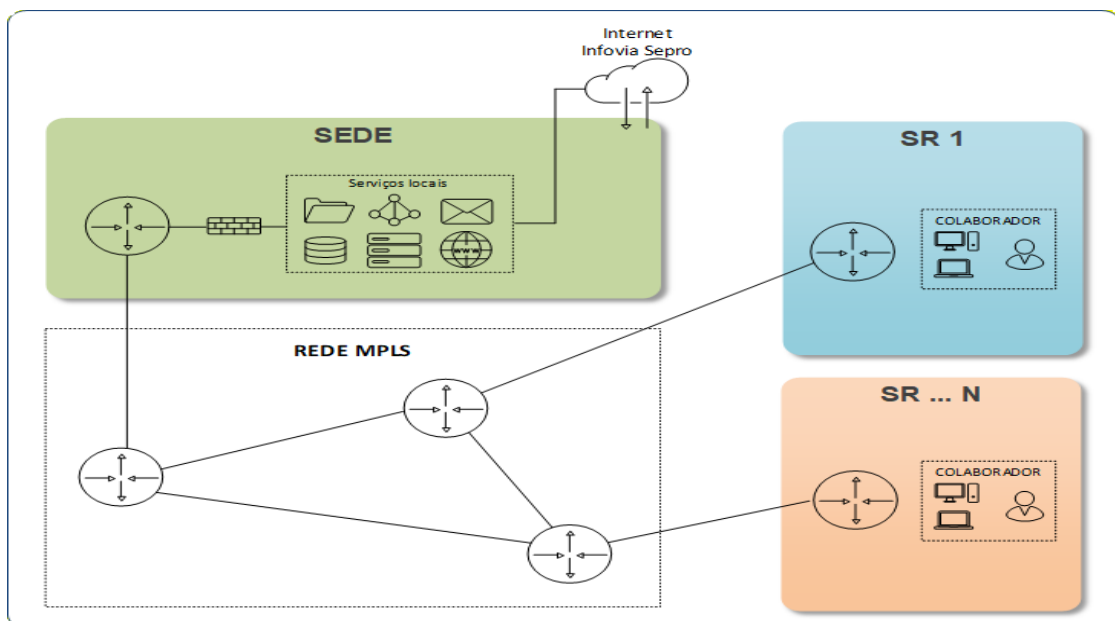


Figura 3: Conexão de rede MPLS e saída a internet.

3.1.11. A situação atual ambiente se agrava com as questões físicas e logísticas da distribuição de unidades remotas. As SR's são as unidades responsáveis administrativamente pelas UA's, porém a maioria das UA's ficam em localidades muito distantes fisicamente da sua respectiva SR. Essa distância dificulta gestão de tecnologia dessas unidades por parte do órgão. Muitas vezes o próprio INCRA Sede e até mesmo a SR possui dificuldade de locomoção até certas UA's, por isso a gestão descentralizada e não otimizada para essas unidades não beneficia o atual cenário.

3.1.12. No Plano Diretor de TIC 2021-2024 (SEI nº 9793479) do Incra, especificamente no Apêndice A - Relação das Superintendências Regionais e Unidades Avançadas (Página 66), é possível verificar a diversidade de localização das unidades organizacionais e imaginar as diversas dificuldades para entregar serviços de TIC com a mesma qualidade que é ofertada na Sede.

3.1.13. Algumas localidades regionais do INCRA, possuem uma pequena infraestrutura de TI (geralmente, mas não se limitando, as SR's) onde utilizam algumas aplicações locais, além de consumirem aplicações localizadas e providas pelo INCRA Sede. Essas aplicações executadas fora do datacenter do INCRA Sede, e mantidas por equipes locais nas unidades remotas, não são, por vezes, aplicações homologadas, o que dificulta a manutenção destas soluções e o acompanhamento dessas dentro dos programas de melhores práticas e ciclo de vida de aplicações.

3.1.14. Assevera-se, ainda, que em casos de falha do link MPLS ou interrupção nos serviços por parte da operadora (visto que há apenas uma operadora fornecendo a conectividade) e no ano de 2021 ocorreram vários casos de inoperância do link, além dos serviços de aplicações e dados ficarem inacessíveis para todas as SR's, fica também indisponível o acesso à internet, já que todos os acessos à Internet por parte dos usuários das SR's são fornecidos e geridos pelo INCRA Sede. As SR's não possuem link de internet, apenas conexão MPLS com a Sede, então, uma vez que as SR's estão conectadas à Sede, o fluxo de acesso a rede passa a ser analisado por esta, realizando controles conforme políticas estabelecidas. Estes acessos utilizam a conexão de Internet contratada pelo INCRA e fornecido pelo Serpro, chamado de INFOVIA, tal conexão possui capacidade de banda de 1Gbps para ser distribuída entre as diversas unidades do INCRA, porém, limitada à estrutura física (capacidade) de entrega dos links MPLS para cada unidade. Logo, a rede INFOVIA é de 1Gbps, mas se uma superintendência/unidade avançada está conectada a um link de MPLS de 12Mbps, a Internet será limitada à no máximo 12Mbps, e não 1Gbps.

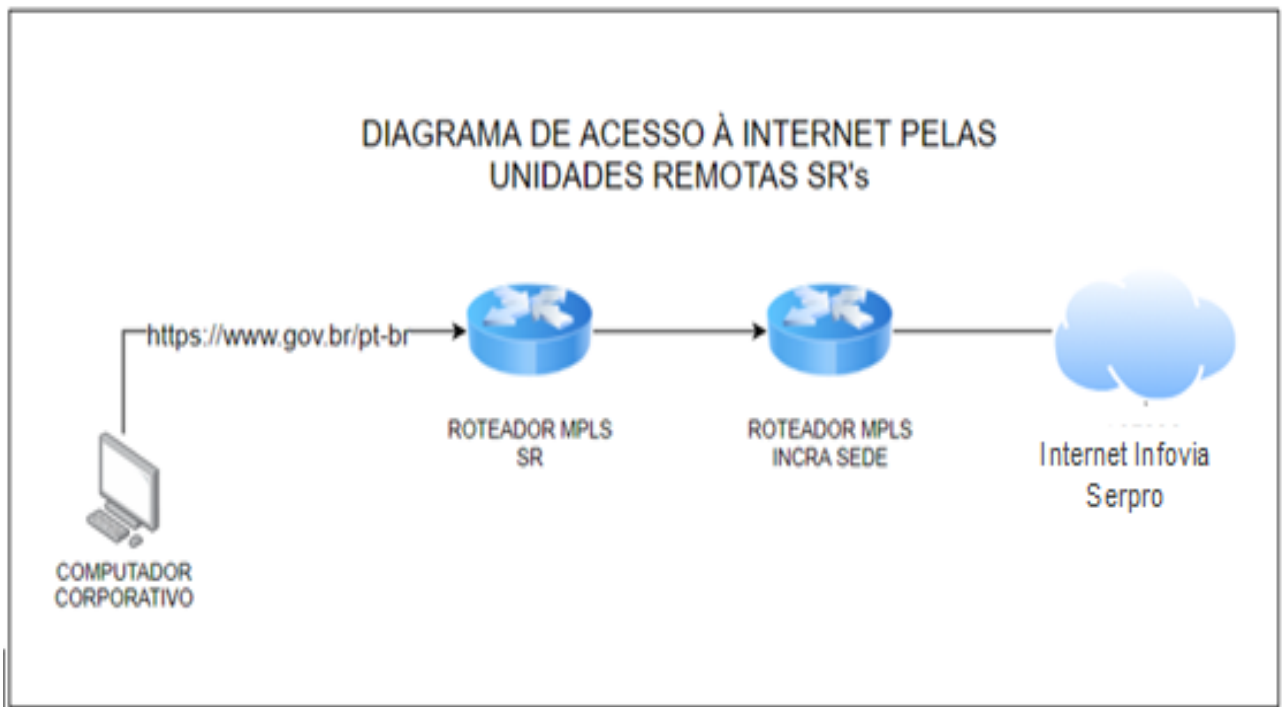


Figura 4: Conexão de acesso à internet por parte das SR's.

3.1.15. O INCRA possui domínio de rede único, ou seja, todos os servidores/colaboradores, estando eles na Sede, SR, UA ou UAE, utilizam usuário de rede e de e-mail com domínio @incra.gov.br. Essa integração na prática traz benefícios claros para a gestão sobre as contas de usuários, uma vez que não há mais necessidade de utilizar domínios distintos para cada localidade. Porém, esse mesmo benefício pode por vezes ser impactado pela já citada fragilidade da conexão entre as unidades e a Sede, já que para existir um domínio único, deve-se haver conectividade estável e redundante entre as unidades.

3.1.16. As Unidades Avançadas (UA) são unidades sem infraestrutura de datacenter e que não possuem conexão do tipo MPLS. Essas unidades utilizam de conexão de Internet comum, geralmente contratada por sua respectiva SR a qual está vinculada. Em alguns casos, as UA's ficam localizadas dentro de outros órgãos ou dependências públicas, utilizando nesses casos de conexão à Internet contratada por este local para acesso via VPN (quando necessário) aos recursos localizados no INCRA Sede. Quando um usuário de uma UA está conectado via VPN com o INCRA Sede, seu acesso à Internet passa a ser gerido pela Sede, porém, quando não utilizando esta conexão VPN, seu acesso à Internet acontece diretamente através de seu link local, não possuindo controle algum de segurança ou de análise de dados, o que compromete e muito o nível de gestão sobre estas unidades.

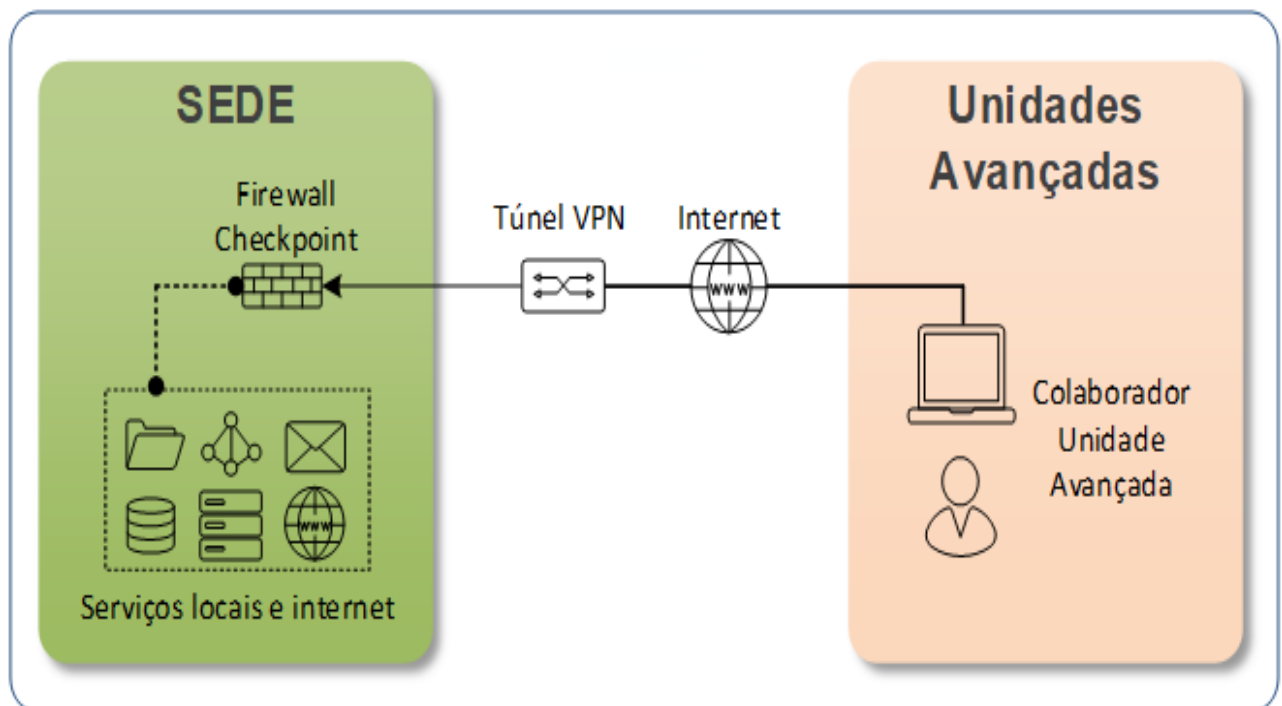


Figura 5: Conexão de usuários colaboradores das UA's.

3.1.17. Tanto a conexão de acesso via VPN, quanto a gestão de acesso à Internet, são geridas pelo INCRA Sede utilizando solução de controle e proxy de acesso à rede baseado no Firewall.

3.1.18. A rede MPLS possui hoje baixa velocidade e disponibilidade de banda de rede, possuindo variação de 4MB a 16MB, e por vezes não suportando a quantidade de usuários necessária com a qualidade e estabilidade devida. As SR's vêm sofrendo frequentemente com problemas de congestionamentos e falhas sobre estes links. Com a questão do congestionamento dos links gera problemas de conexão e dificuldade nas ações cotidianas por parte dos colaboradores dessas unidades, evidenciando a precariedade do serviço. Esta situação pode ser evidenciada através de histórico de processos SEI listados a seguir, apenas para exemplificar tal situação. Lista-se ainda, UA's que se quer possuem o serviço contratado, sofrendo por vezes de grandes problemas e ainda não utilizando do benefício da centralização, conectividade e controle.

- Unidade SR (27) – Marabá – Processo SEI 54000.048097/2021-01 e 54000.086057/2021-50, em especial o documento Relatório (SEI nº 9949147);
- Unidade SR (12) – Maranhão – Processo SEI 54000.025215/2021-03;
- Unidade SR (12) – Maranhão – UA-12.5 Barra do Corda – não possui o serviço contratado;
- Unidade SR (12) – Maranhão – UA-12.6 Zé Doca – não possui o serviço contratado;
- Unidade SR (16) – Mato Grosso do Sul – UA-16.1 Dourados – não possui o serviço contratado;
- Unidade SR (25) – Roraima – UA-25.3 Rarainópolis – não possui o serviço contratado;
- Unidade SR (06) – Minas Gerais – Processo SEI 54000.071501/2019-18;
- Unidade SR (26) – Tocantins – Processo SEI 54000.002663/2021-21;
- Unidade SR (30) – Santarém – UA-30.2 Miritituba - Itaituba – não possui o serviço contratado.
- Unidade SR (30) – Santarém – UA-30.6 Rurópolis – não possui o serviço contratado.

3.1.19. No cenário atual os dados e aplicações estão descentralizados, ou seja, as unidades consomem recursos de tecnologia providos pelo INCRA Sede e (algumas localidades) possui também sua própria infraestrutura de TI com suas aplicações armazenadas e executadas localmente. A falta de centralização ocasiona em alguns problemas como a dificuldade no gerenciamento, já que cada unidade, quando há, possui pequena e precária equipe de TI. As aplicações, por estarem descentralizadas, sofrem de problemas de falta de capacidade de gestão, dificuldade de suporte aos usuários remotos, dificuldade de aplicação de políticas de segurança de acesso remoto, etc.

3.1.20. A controladoria Geral da União – CGU, possui recomendações sobre a centralização de dados e a não utilização de tecnologia descentralizadas (quando os dados estão espalhados em várias unidades). A recomendação se baseia no princípio de citado acima, onde problemas relacionados à dados e falhas de aplicação se tornam um enorme empecilho tecnológico para a transformação digital e evolução tecnológica, além da necessidade de manter datacenters espalhados em várias localidades, gerando custos altos de aquisição e manutenção dos mesmos.

"Sistema e-Aud CGU - Recomendação 25: Normatizar a proibição de TIs paralelas criadas sem a participação e consentimento da DOT e estabelecer que todas as demandas de TI sejam submetidas à aprovação prévia do Comitê de Segurança e Tecnologia da Informação. (Refere-se ao achado F.13)" (GRIFO NOSSO)

3.1.21. Foi definido como status atual, a falta de centralização de dados e a fragilidade da malha de conexão de rede entre a Sede e as unidades remotas. Desta forma, caracteriza-se que as duas camadas de tecnologia estão diretamente conectadas, uma vez que o fator determinante para que a descentralização seja o status atual neste órgão, é a camada de conectividade.

3.2. A solução atual de conectividade de unidades remotas e centralização de dados, encontra-se na fase 4 "Ciclo de vida dos ativos de TI" de acordo com o documento "BOAS PRÁTICAS, ORIENTAÇÕES E VEDAÇÕES PARA CONTRATAÇÃO DE ATIVOS DE TIC – Versão 4" (https://www.gov.br/governodigital/pt-br/contratacoes/orientacoes_ativos-de-tic-v-4.pdf). Todavia, a inicialmente, parte de conectividade de links será mantida e expandida através deste processo. Já a solução de acesso remoto torna-se depreciada para o uso aberto aos usuários, sendo novamente dedicada para seu propósito inicial, acessos pontuais por parte da equipe de TI, principalmente.

"1.1. ESCOLHA DO POSICIONAMENTO ADEQUADO DA TECNOLOGIA

1.1.1. Para se garantir economicidade nas aquisições de ativos de TI, deve-se buscar definir as especificações técnicas de modo a posicionar a aquisição adequadamente dentro do ciclo de vida do bem.

1.1.2. De forma geral, o ciclo de vida dos ativos de TI obedece a quatro fases, a saber:

Fase 1: Lançamento.

Nesta fase, os ativos de TI são naturalmente mais caros por representarem produtos recentemente lançados no mercado e que encontram-se na vanguarda da tecnologia. Normalmente há poucas opções de fornecedores disponíveis no mercado e alguma dificuldade na manutenção e reposição.

A aquisição de ativos de TI nesta fase do ciclo de vida deve pautar-se na justificativa da necessidade de provimento de serviços altamente diferenciados em desempenho e/ou capacidade e que não possam ser providos por ativos que se encontrem na fase de Menor Custo ou alternativamente na fase de Seleção.

Fase 2: Seleção.

Fase imediatamente posterior à de Lançamento, na qual os ativos de TI têm menor custo se comparados à fase anterior, alta capacidade de customização e níveis crescentes de padronização e de suporte de mercado. A estratégia de aquisição dos ativos de TI deve contemplar, via de regra, os bens que estejam compreendidos na fase Menor Custo ou alternativamente nesta fase, levando-se em consideração as necessidades de desempenho e/ou capacidade, a vida útil prevista para o equipamento, entre outros.

Fase 3: Menor Custo.

Fase imediatamente posterior à Seleção, neste momento os ativos de TI estão altamente comoditizados, atingindo seu menor custo de comercialização, tanto para aquisição como para manutenção, possuem alta capacidade de customização, alta padronização e adequado suporte de mercado. A estratégia de aquisição dos ativos de TI deve contemplar, preferencialmente, os bens que estejam compreendidos nesta fase de melhor relação custo / capacidade ou alternativamente na fase Seleção, levando-se em consideração as necessidades de desempenho e/ou capacidade, a vida útil prevista para o equipamento, entre outros.

Fase 4: Substituição.

Fase imediatamente posterior a Menor Custo, representa a última no ciclo de vida dos bens de TI. Normalmente, os ativos de TI nesta fase têm baixa comercialização e alto custo de manutenção. São compostos normalmente pelos ativos que fazem parte do legado tecnológico da instituição. A estratégia de aquisição dos ativos de TI deve ser trabalhada de forma a implementar uma política de substituição e descarte, conforme item 1.3 deste documento, visando não incorrer em custos elevados de manutenção de tecnologia já obsoleta." (GRIFO NOSSO)

3.3. Cenário de acesso para mobilidade e trabalho remoto

3.3.1. Além da fragilidade da malha de conectividade do INCRA Sede com as demais unidades, cita-se também a problemática de conexão de trabalho remota para os servidores/colaboradores, pois agravado pela pandemia do COVID-19, esse modelo tem se tornado extremamente necessário. Porém não basta apenas permitir que o colaborador acesse remotamente seus dados e aplicações, torna-se necessário trazer uma usabilidade eficiente e completa para a mobilidade e trabalho remoto, e ainda manter a experiência do usuário quando ele eventualmente estiver realizando suas atividades dentro das dependências do INCRA.

3.3.2. Não é desnecessário repisar que os acessos remotos dos servidores/colaboradores se dão por meio de conexão VPN (Virtual Private Network), utilizando-se da solução de Firewall atual de marca Checkpoint. Uma conexão VPN estabelece uma conexão criptografada entre o usuário e o datacenter do INCRA. Esse acesso se dá por meio de aplicação cliente instalado no dispositivo do usuário, e esse dispositivo passa a ser um dispositivo dentro da rede do cliente, e acessando suas aplicações como se estivesse dentro do escritório. Esse tipo de conexão atualmente é feito pelos servidores/colaboradores das unidades remotas quando necessário e também pelos servidores/colaboradores quando externos, atuando em teletrabalho ou trabalho remoto, quando fora do escritório, devido ao cenário atual da pandemia, onde o INCRA e diversos órgãos do governo federal tiveram que enviar colaboradores para casa e houve a necessidade de prover solução que permitisse o acesso às aplicações, independente do lugar em que o usuário está.

3.3.3. Uma conexão VPN estabelece uma conexão criptografada, chamada de "conexão segura" entre o usuário e o INCRA (client-to-site). Por meio da VPN, todo o tráfego de dados é roteado por um túnel virtual criptografado.

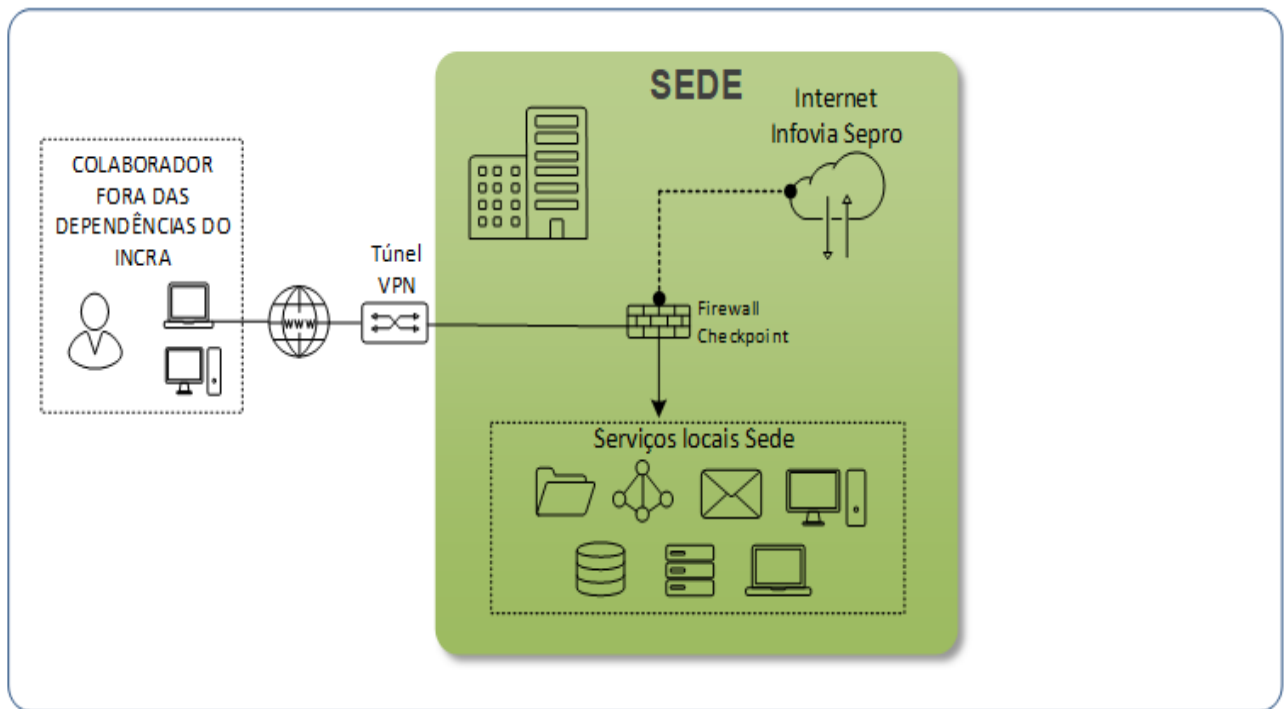


Figura 6: Modelo de conexão via VPN para colaborador em teletrabalho.

3.3.4. A conexão por meio de um Cliente VPN, torna o usuário capaz de acessar recursos computacionais dentro do datacenter do INCRA. No cenário atual, quando um usuário é servidores/colaborador de uma SR, ele se conecta através da conexão MPLS já estabelecida, utilizando recursos nativamente sem a necessidade de estabelecer um túnel VPN.

3.3.5. A solução de VPN não é um meio de conexão para amplo acesso remoto, por muitas vezes inclusive, não entregando boa experiência e estabilidade de conexão aos usuários, e não suportando grandes quantidades de usuários conectados ao mesmo tempo. Tal solução não foi desenvolvida para esse fim, sendo criada especificamente para acessos pontuais, principalmente para as equipes de TI/Segurança. Quando há uma necessidade de alta carga de usuários, os equipamentos que realizam conexões VPN são impactados, justamente por não serem desenvolvidos para uma massiva e simultânea quantidade de acessos. Com esse impacto, a experiência do usuário é degradada, impactando na sua produtividade, por conta dos frequentes problemas de conectividade (quedas de sessão), falhas na entrega de aplicações, alto tempo de resposta etc. A solução de VPN, conhecida por não ser a forma mais segura de acesso remoto. Esta afirmação é evidenciada pelos recentes ataques a entidades governamentais divulgado na mídia. A cerca desta solução, é importante ressaltar alguns outros pontos de problemática, como a seguir:

3.3.5.1. Em caso de comprometimento da máquina do usuário, a rede do órgão fica vulnerável a ataques como DDoS (*Distributed Denial of Service* – Ataque de Negação de Serviço) por exemplo;

3.3.5.2. A administração de filtros de acesso dentro do contexto “seguro” da VPN é complexa e onerosa em tempo e não muito prático para o usuário do ponto de vista de usabilidade;

3.3.5.3. Soluções de conformidade da máquina do usuário são necessárias para mitigar o risco mencionado acima, com isso fica restrito a utilização do ambiente a dispositivos do órgão ou em *compliance*, dificultando aplicações de políticas em dispositivos pessoais, muitas vezes necessários para acesso ao ambiente via VPN;

3.3.5.4. As informações do órgão trafegam entre a máquina do usuário que se encontra “fora do ambiente tecnológico” e o servidor localizado na Infraestrutura de TI do INCRA;

3.3.5.5. É necessário muito mais recursos de rede (largura de banda) tanto do lado do dispositivo como do lado do Data Center para suportar todo o tráfego;

3.3.5.6. Apesar de ser uma conexão denominada “criptografada”, a conexão abre uma “porta” para ataques externos e se torna totalmente dependente da segurança do dispositivo do usuário, que por muitas vezes está desatualizado e sem proteção, acarretando brechas enormes de segurança por colocar o usuário dentro da infraestrutura de TI no INCRA e consequentemente colocando um possível invasor ou entidade maliciosa também nessa mesma infraestrutura.

3.3.5.7. Aplicações mais sensíveis enfrentam problemas de desempenho, pois a VPN historicamente não é uma conexão com alta capacidade de resiliência e muito sensível a qualquer problema ou queda de conexão.

3.3.6. Quando os usuários estão externamente, ou seja, fora de qualquer unidade remota ou da Sede, sempre é utilizado a conexão via VPN. Esses usuários necessitam de instalar o cliente VPN em seus computadores, sejam eles corporativos ou não, e realizar a configuração deste componente. Essa configuração geralmente é feita por meio das equipes de TI, sejam elas da Sede ou das SR’s (quando se tratar de uma UA).

3.3.7. Além dos servidores/colaboradores em trabalho remoto, utilizam-se da VPN os servidores/colaboradores que se encontram dentro das unidades avançadas. Esses usuários acessam via conexão VPN o ambiente de TI da Sede, uma vez que esses locais não possuem conexão do tipo MPLS.

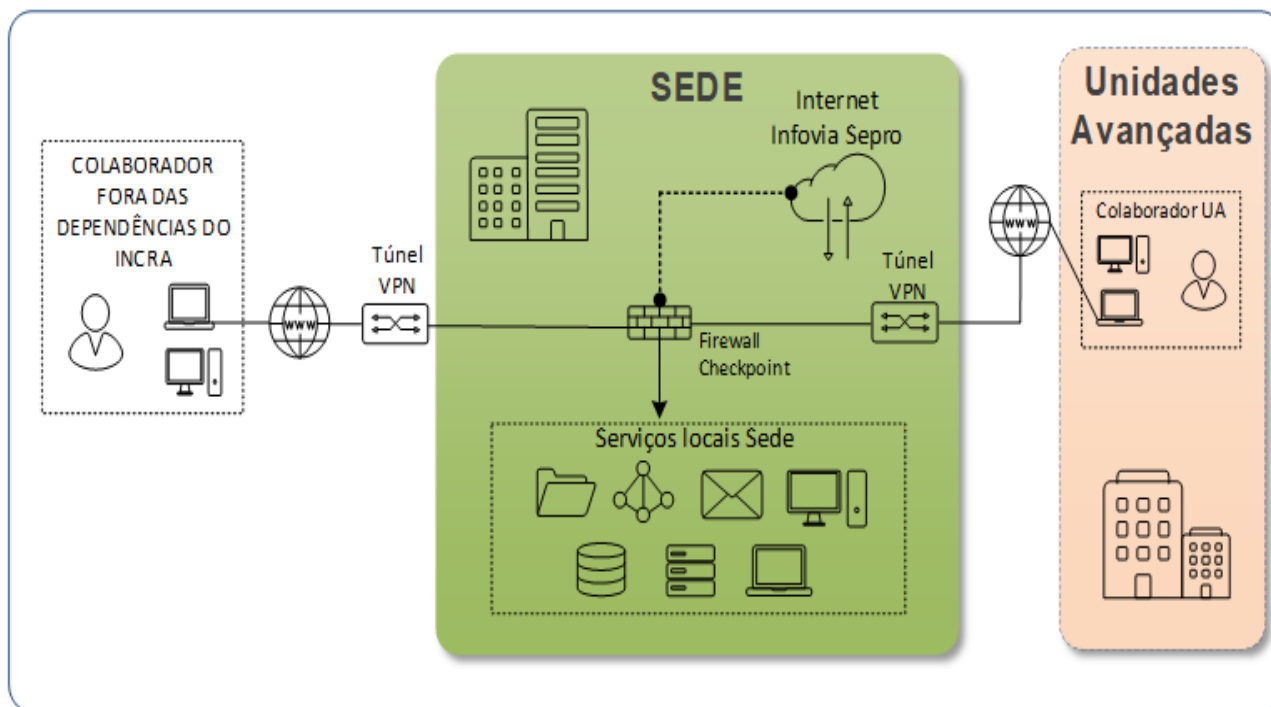


Figura 7: Modelo de acesso colaborador em teletrabalho e colaborador da UA.

3.3.8. Nesse contexto, percebe-se outro dificultador da manutenção do modelo de acesso atual, é a utilização de sistemas legados, como por exemplo a aplicação SIPRA. O SIPRA, assim como alguns outros sistemas, possui características específicas para ser executado, como por exemplo, versão específica e antiga do **browser Internet Explorer (IE versão 11)**, não sendo possível de ser acessado por outros browsers. Para o acesso à essa aplicação citada, é necessário também uma versão específica e antiga de JAVA, habilitação de modo de compatibilidade e entre outras especificidades necessárias às suas execuções. As aplicações e sistemas geralmente são atualizadas por seus desenvolvedores para corrigirem problemas ou falhas de segurança, então estas especificidades acarretam problemas de segurança para o órgão, visto que, por exemplo, o JAVA e o Internet Explorer devem estar em versões desatualizadas e passíveis de corrupções. Vale lembrar que o Internet Explorer está sendo descontinuado pela Microsoft para algumas versões de sistema operacional. Estima-se que o desenvolvimento de uma nova aplicação para substituição do SIPRA, levaria em torno de 12 meses, o que acarretaria um custo considerável ao órgão ou até ser absorvido pela Plataforma de Governança Territorial - PGT, e ainda não resolveria as demais aplicações desatualizadas, além de tornar necessário ainda mais atualizações ao longo do tempo. Neste modelo, torna-se necessário ainda que os dispositivos utilizados pelos usuários se mantenham atualizados em requisitos técnicos e que possuam poder computacional adequado ao seu perfil de uso de aplicações. Essa abordagem nem sempre é passível de ser validada uma vez que o INCRA não é detentor de todos os dispositivos utilizados pelos colaboradores, sendo por vezes utilizado para acesso, dispositivos pessoais, quando o colaborador está em trabalho remoto.

3.3.9. Há uma série de aplicações hoje providas pelo INCRA, que já estão ou serão centralizadas, e que necessitam de acesso seguro por parte dos servidores e colaboradores, estejam eles externos (em trabalho remoto) ou internos (dentro das unidades remotas e da sede). Estas aplicações serão disponibilizadas conforme perfil de cada uma para os usuários ou grupos de usuários pertinentes a estes perfis. A seguir, a lista de aplicações em rol não taxativo:

- 3.3.9.1. Banco de Dados / QGIS
- 3.3.9.2. e-pessoal TCU
- 3.3.9.3. e-Siape
- 3.3.9.4. Incranet
- 3.3.9.5. Microsoft Office 365
- 3.3.9.6. Sala da Cidadania
- 3.3.9.7. SCDP
- 3.3.9.8. SEI (Sistema Eletrônico de Informações)
- 3.3.9.9. SIP (Sistema de Permissões)
- 3.3.9.10. SIAFI Tesouro
- 3.3.9.11. HOD Serpro
- 3.3.9.12. SIAPENET
- 3.3.9.13. Siconv (Sistema de Gestão de Convênios e Contratos de Repasse do Governo Federal)
- 3.3.9.14. SIGAC / SIGEPE
- 3.3.9.15. SIGEF (Geo)
- 3.3.9.16. SIGEF (Titulação)
- 3.3.9.17. SIGEF (Homologação)
- 3.3.9.18. SIGEF (Resultados)
- 3.3.9.19. SIPRA
- 3.3.9.20. SIPRA (Consulta)
- 3.3.9.21. Sistema de RME
- 3.3.9.22. SCP - ASI

- 3.3.9.23. SISPROT
- 3.3.9.24. SNCCI
- 3.3.9.25. SNCR
- 3.3.9.26. TDCalc
- 3.3.9.27. Vólus
- 3.3.9.28. Zabbix
- 3.3.9.29. Zimbra Admin

3.3.10. O uso da VPN expande ainda mais essa complexidade, visto que o dispositivo do usuário por vezes pode não estar atualizado, e uma vez que o usuário está com uma conexão direta ao datacenter do órgão, este por sua vez, também se torna vulnerável.

3.3.11. Durante a pandemia foi necessário adotar o modelo de trabalho remoto (*home-office*) com maior amplitude, atendendo às recomendações dos órgãos de saúde e mantendo os colaboradores seguros. O atendimento às necessidades tecnológicas nesse momento foi feito por meio da entrega de acesso VPN a esses colaboradores. A demanda de usuário ao modelo de teletrabalho cresceu absurdamente e, como explanado anteriormente, as soluções de VPN não foram concebidas para receber grande demanda de usuário, carregando ainda mais o fluxo de dados dentro do INCRA, além de não permitir uma gestão avançada de ameaças e um suporte otimizado ao usuário. A liberação do trabalho remoto aos colaboradores traz a necessidade de uma solução de espaço de trabalho virtual (*workspace*), que permita o uso de aplicações e dados de forma remota, virtual, segura e disponível, algo que atualmente não é realizado no INCRA.

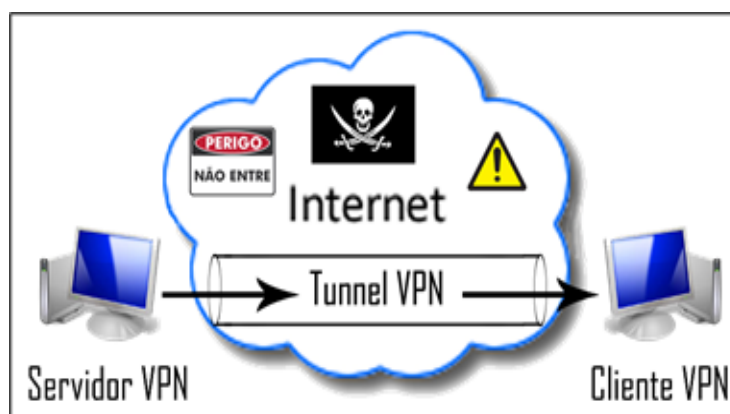


Figura 8: Riscos da conexão VPN.

3.3.12. Para que os dados e aplicações estejam ligeiramente mais seguros, o dispositivo utilizado pelo usuário para acesso via VPN, precisa estar sempre atualizado a fim de evitar ataques e invasões, que por sua vez pode tornar vulnerável a conexão do usuário e afetar a segurança das aplicações e dados do INCRA. Com este tipo de tecnologia necessita de uma ação muito forte e desgastante por parte do INCRA para tentar manter esses dispositivos e a conexão segura. Uma vez que o usuário está utilizando seu dispositivo pessoal para acesso ao ambiente do INCRA, essa gestão se torna ainda mais deficitária, já que não muitas ações passíveis de se tomar sobre dispositivos pessoais e não geridos pela instituição.

3.3.13. Deve-se destacar o fato de que o serviço de VPN, além de ser de difícil gerenciamento pela TI, muitas vezes apresenta instabilidades, o que prejudica os trabalhos dos servidores que dele dependem. Outros pontos negativos são: 1) A necessidade de que, por vezes, os colaboradores deixem seus dispositivos (computadores) ligados dentro das dependências do INCRA para o acesso externo (utilizando o protocolo RDP após a conexão VPN), o que gera um consumo desnecessário de energia elétrica e diminui a vida útil dos equipamentos. 2) A dificuldade da área de TI oferecer suporte aos servidores que estão trabalhando remotamente.

3.3.14. A problemáticas de conectividade apresentadas se arrasta sobre dois principais prismas, sendo estes:

1. A grande fragilidade de conexão de rede das unidades remotas, possuindo estas apenas um link de conexão e necessitando consumir recursos do INCRA Sede através deste falho e único recurso.
2. A descentralização de dados e aplicações fora do INCRA Sede, trazendo a dificuldade de controle, aplicação políticas de segurança e melhores práticas, além de tornar necessário que as unidades remotas mantenham em suas dependências a necessidade de gerir um datacenter (Centro de Processamento de Dados - CPD) onde executam estas aplicações não homologadas. Essa abordagem de centralização de dados, gera a necessidade de entregar acesso remoto as aplicações e dados centralizados no INCRA Sede.

3.4. Entende-se que atualmente o INCRA possui cenário desafiador e as mudanças que serão apresentadas neste documento são de extrema importância para a continuidade do fornecimento de tecnologia e soluções e aprimoramento da qualidade por parte do INCRA às suas entidades. O perfeito cenário de utilização de aplicações e dados, seria a centralização e a distribuição/manutenção destes serviços por parte do INCRA Sede, já que essa entidade, possui quadro amplo de servidores/colaboradores especializados para garantir a qualidade de atendimento desses serviços. Além da centralização, torna-se necessário a inclusão de redundância e alta disponibilidade de conectividade para todas as unidades remotas SR's e UA's.

3.5. O cenário do acesso remoto e descentralização do INCRA embute riscos também à segurança das informações geridas por esta entidade, estes riscos estão diretamente relacionados ao transporte de informações e aos equipamentos utilizados por parte dos colaboradores, não fornecidos e não certificados pelo INCRA Sede, assim com a centralização, acesso remoto e conectividade redundante, busca-se acrescentar uma camada de segurança de acesso à rede de dados do INCRA independentemente do equipamento utilizado, local de acesso e aplicação consumida, a fim de se propiciar aos colaboradores acesso integral aos recursos necessários para a produção de suas atividades.

4. SOLUÇÃO PROPOSTA – QUANTIDADE DE BENS E SERVIÇOS (IN SGD/ME Nº 01/2019, ART.11, INCISO I)

4.1. DESCRIÇÃO SUCINTA

4.1.1. Aquisição de **solução de espaço de trabalho virtual** atendendo aos padrões nacionais e internacionais de segurança de dados, agregando produtividade e facilitando o atendimento de suporte aos colaboradores.

4.1.2. Aquisição de **solução de agregação e balanceamento de links** com inteligência avançada de redundância e entrega de pacotes.

4.1.3. Aquisição de **serviço de link de internet redundante** para as unidades remotas.

4.1.4. Analisa-se a solução para o período de 12 meses, renováveis até 60 meses.

4.1.5. Tendo como característica a redução de custos, a centralização permitirá que os datacenters espalhados por todo Brasil, constantes na SR's e UA's, deixem de ser necessários, e consequentemente seu custo de aquisição, manutenção de equipamentos e sala de datacenter, softwares, suporte e garantia. Com este projeto ainda, as SR's e UA's se beneficiarão com a alta disponibilidade, que está presente no datacenter do INCRA Sede, e permitirá que as aplicações e dados ali presentes, estejam sempre disponíveis aos colaboradores através de conexão otimizada e redundante para SR e UA compatíveis com SR em tamanho e número de usuários.

4.1.6. Visando a melhoria na entrega dos serviços, e para que a centralização das aplicações e dados se torne viável junto à solução para espaço de trabalho virtual, foi considerado neste estudo funcionalidades de agregação e balanceamento de links, baseado em *appliance* física de solução de SD-WAN para conectividade e alta disponibilidade, e link extra de internet, que foi considerado neste projeto. A solução de SD-WAN criar uma rede WAN virtual capaz de integrar e conectar sites tecnológicos através de links de internet. A solução de conectividade e a solução de espaço de trabalho virtual juntas, permite que os colaboradores possam utilizar suas aplicações e dados de qualquer lugar (estando dentro ou fora das dependências do INCRA), utilizando qualquer dispositivo (mesmo que não gerenciado pelo INCRA) e ainda permitindo que o INCRA entregue suas aplicações mais antigas e desatualizadas com alta segurança e disponibilidade de conexão, evidenciando a melhora na experiência e produtividade dos colaboradores.

4.1.7. A utilização da solução de espaço de trabalho virtual com agregação e redundância de links, torna-se extremamente vantajosa também, pela não necessidade de adequação de tecnologia de datacenter do INCRA, sendo essa possível de se executar sob qualquer solução de processamento, armazenamento e virtualização de servidores, por isso mantem-se as soluções já adquiridas pelo INCRA e consequentemente seu investimento.

4.1.8. A solução será amplamente utilizada em conjunto com as unidades remotas, para que todos os acessos sejam centralizados e administrados pelo INCRA Sede. Por isso o INCRA planeja uma contratação de solução para Espaço de Trabalho Virtual com agregação de links, conectividade redundante e disponibilidade de acesso, sendo divididos em grupos, da seguinte forma:

GRUPO 1			
ITEM	DESCRIÇÃO	UNIDADE	QUANTIDADE
1	Solução de Espaço de Trabalho Virtual	Usuário	6000
2	Implantação e Repasse de Conhecimento	Serviço	01
GRUPO 2			
ITEM	DESCRIÇÃO	UNIDADE	QUANTIDADE
1	Agregação e Balanceamento de Links Tipo 1 (UNIDADES REMOTAS)	Appliance	77
2	Agregação e Balanceamento de Links Tipo 2 (SEDE)	Appliance	02
3	Implantação e Repasse de Conhecimento	Serviço	01
GRUPO 3			
ITEM	DESCRIÇÃO	UNIDADE	QUANTIDADE
1	Link de Internet 01 - 20Mbps	Link	77
2	Link de Internet 02 - 20Mbps (Redundante)	Link	77**

*Estimativa com base no atual número de usuários.

** Nem todas as Unidades Avançadas terão link redundante, pois existem UA que são

Tabela disposição de itens para aquisição.

4.1.9. A quantidade prevista para o GRUPO 1 foram baseadas na quantidade de colaboradores ativos do INCRA passíveis de utilização da solução de espaço de trabalho virtual. A quantidade prevista para os GRUPOS 2 e 3 foram baseadas no somatório das unidades remotas (SR's, UA's e UAE's) que utilizarão da solução de conectividade, agregação e balanceamento de links, sendo que todas as SR's terão link redundante e algumas Unidades Avançadas, haja vista que existem UA's com menos de 05 usuários e ainda há histórico de mudança de localidade das Unidades Avançadas e por isso já se projeta o uso de Registro de Preço para esta pretensa contratação, em especial quanto ao fato de não ser possível definir previamente e com a devida precisão o quantitativo de unidades que poderão sofrer modificação ou não ter redundância link.

4.1.10. Está previsto a possibilidade de aumento de velocidade nas conexões dos links, de até o dobro da velocidade contratada, sendo a CONTRATADA responsável por manter suporte ao dobro de velocidade, totalizando 40Mbps para cada link. São 77 unidades totais, cada uma receberá 2 links de Internet, com isso, como estão sendo previstos 2 itens dentro do GRUPO 3.

4.2. SOLUÇÃO DE ESPAÇO DE TRABALHO VIRTUAL

4.2.1. Solução para espaço de trabalho virtual, para acesso às aplicações, desktops e dados virtualizados, de acordo com as especificações do Anexo I – ETPC (10012570).

4.2.2. Justificativas.

4.2.2.1. As tecnologias de espaço de trabalho virtual, constituem alternativas tecnicamente viáveis à utilização de VPN ou qualquer outro modelo de acesso para trabalho remoto. Estas soluções permitem que colaboradores acessem dados, sistemas e aplicativos importantes de sua organização a partir de diversos dispositivos e de diferentes locais, mantendo ainda a experiência onde quer que ele esteja, seja dentro das dependências do órgão ou em casa.

4.2.2.2. Dentre as vantagens das soluções que podem ser utilizadas alternativamente à VPN, podemos listar:

- Aderência ao modelo de trabalho remoto e transformação digital;
- Gerenciamento centralizado de dispositivos;
- Entrega de aplicações de forma altamente segura;
- Controle de políticas de usuários baseados em perfis;
- Rápida implantação;
- Agilidade de acesso às aplicações e dados;
- Redução de necessidade de suporte a estações físicas;
- Implantação padronizada e centralização de dados e aplicações;
- Aumento da segurança;
- Possibilidade de disponibilizar ambientes para treinamentos ou eventos, substituindo a necessidade de configuração de diversos desktops físicos;
- Realização de serviços técnicos fora do expediente;
- Atendimento aos padrões e regulamentos de segurança da informação e dados;

- Acesso durante deslocamentos entra as unidades remotas quando necessário.

- 4.2.3. O aumento vertiginoso do acesso remoto devido à pandemia do COVID-19, robusteceu ainda mais a necessidade de minimizar os riscos de vazamento, a perda de informações e os ataques à rede interna do INCRA.
- 4.2.4. A tecnologia de espaço de trabalho virtual é justificada, pois apresenta variáveis de desempenho (performance de conexão, experiência de usuário, alta disponibilidade, etc.) melhores que a solução de acesso remoto atual, e ainda, habilita as unidades remotas à acessar os dados e aplicações do INCRA de forma centralizada e organizada, principalmente ao se comparar com outras soluções tradicionais como acesso via VPN, que demandariam altos níveis de suporte, e aquisição de softwares extras como softwares de gerenciamento da máquina do usuário e segurança de arquivos.
- 4.2.5. Além das características supracitadas, a solução permitirá ao INCRA criar aderência ao modelo de Teletrabalho, onde colaboradores podem realizar suas atividades de forma remota ao escritório, sendo esse espaço remoto uma SR ou UA, ou até mesmo sua própria residência. O teletrabalho é um modelo real e que tem se tornado uma tendência na Administração Pública Federal - APF, e também no mercado, pois já é previsto legalmente pelo TST, segundo o Artigo 6º da Consolidação das Leis do Trabalho (CLT), que afasta as distinções entre o trabalho realizado no estabelecimento do empregador, o executado no domicílio do empregado e o realizado a distância, desde que estejam caracterizados os pressupostos da relação de emprego. O parágrafo único do dispositivo, introduzido em 2011, estabelece que “os meios telemáticos e informatizados de comando, controle e supervisão se equiparam, para fins de subordinação jurídica, aos meios pessoais e diretos de comando, controle e supervisão do trabalho alheio”.
- 4.2.6. A Reforma Trabalhista (Lei 13.467/2017) introduziu um novo capítulo na CLT dedicado especialmente ao tema: Capítulo II-A, “Do Teletrabalho”, com os artigos 75-A a 75-E). Os dispositivos definem o teletrabalho como “a prestação de serviços preponderantemente fora das dependências do empregador, com a utilização de tecnologias de informação e de comunicação que, por sua natureza, não se constituam como trabalho externo”.
- 4.2.7. Existe uma grande e crescente tendência, tanto no poder público quanto na iniciativa privada, acerca da utilização de soluções que implementem o teletrabalho, alguns exemplos de utilização são: CGU, TCU, TST e outros. Com estes exemplos citados, vê-se que a aplicação deste conceito e tecnologias, já é bastante madura e torna mais eficiente o trabalho dos colaboradores.
- 4.2.8. Deste modo, o teletrabalho permitido pelo INCRA e embasado legalmente pelo TST, permitirá que colaboradores realizem suas atividades de forma mais proveitosa, utilizando seu próprio espaço e incidindo em economicidade de recursos físicos ao INCRA, uma vez que o fluxo reduzido de pessoal nas dependências físicas é sabidamente um alto custo. Cita-se também que o próprio TST é usuário de solução para trabalho remoto.
- 4.2.9. Segundo o próprio TST, o teletrabalho entrega benefícios para os colaboradores, tais como: *“Usualmente realizado de casa, o teletrabalho também se adapta a outros lugares, como cafés, ambientes de co-working e até restaurantes. Uma das vantagens é evitar gastos e tempo com deslocamentos e engarrafamentos. A possibilidade de poder trabalhar de qualquer lugar também permite maior flexibilidade e conforto ao trabalhador”*.
- 4.2.10. Um ponto de extrema importância é a mensuração de tópicos referentes às métricas de performance e produtividade dos colaboradores, sendo este necessário para garantir a forma de trabalho dinâmica. Por isso uma característica presente em qualquer projeto dessa modelagem necessita de uma camada de gerência sobre as atividades realizadas por parte dos usuários da solução.
- 4.2.11. A segurança dos dados se torna um assunto cada vez mais abordados em qualquer empresa, seja de administração pública ou privada, pois está diretamente conectado às legislações vigentes acerca da LGPD (Lei Geral de Proteção de Dados). Um ponto avaliado neste projeto, são características de segurança voltada para proteger os dados do INCRA e os usuários de forma bilateral, onde poderá ser segmentado requisitos de acesso às aplicações e dados por parte dos usuários.
- 4.2.12. Por fim, e tecnologia aqui descrita tem o papel primário nessa aquisição, uma vez que essa permitirá que todos os benefícios já citados sejam entregues, e permitam que tudo esteja disponível rapidamente para uso. Vale lembrar que o modelo de trabalho por parte dos colaboradores com a solução de espaço de trabalho virtual torna-se totalmente dinâmico, sendo esse passível de ser realizado por meio de qualquer dispositivo utilizado e em qualquer lugar.
- 4.2.13. Ainda, reforça-se que a solução que complementa tal projeto (agregação e balanceamento de conexão de acesso), traz benefícios aos colaboradores do INCRA que estejam executando suas atividades nas dependências das SR's, UA's ou UAE's, quando estes mesmos usuários estiverem em qualquer outra localidade, como sua casa ou outra unidade do INCRA, o uso de suas aplicações e dados serão os mesmos, trazendo uma excelente experiência unificada aos colaboradores, independentemente do local por onde ele esteja acessando. Os colaboradores em teletrabalho utilizarão sua própria internet para acesso ao portal de trabalho virtual, onde realizará suas atividades diárias de forma segura e com experiência melhorada. Os colaboradores internos, ou seja, estando dentro de algum escritório, seja ele SR, UA, UAE ou a SEDE utilizarão os recursos de rede da unidade organizacional em que estiver, se beneficiando da alta disponibilidade entregue pela agregação e balanceamento de acesso (GRUPO 2) somado aos links redundantes que serão instalados nas unidades remotas (GRUPO 3). Com isso o acesso será feito sempre de forma redundante, disponível e otimizada.

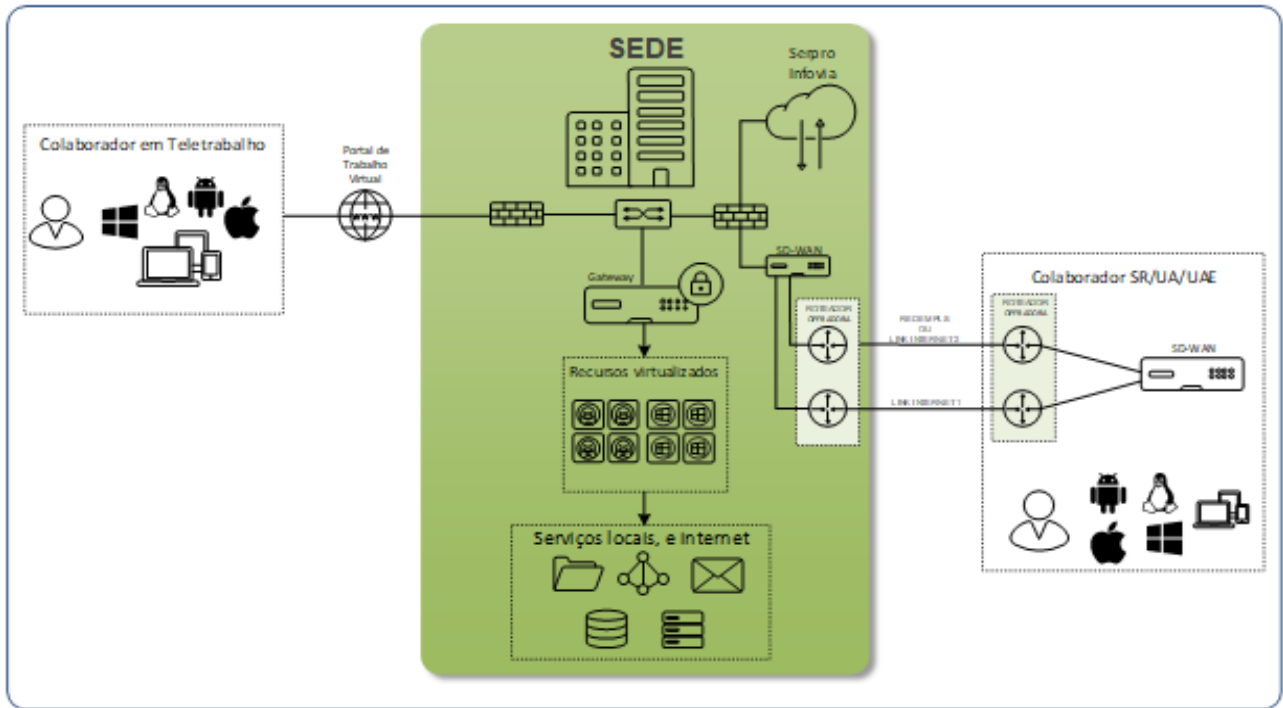


Figura 9: Conexão de colaboradores com solução de espaço de trabalho virtual.

4.2.14. Em diversos casos, ouviu-se falar de invasões e infecções que se iniciaram através de dispositivos de colaboradores remotos conectados via VPN à uma entidade corporativa. Com a solução proposta esses acessos independem da segurança da conectividade e do dispositivo do usuário, já que a solução proverá uma conexão através de protocolo seguro entregando apenas os gráficos das aplicações, e toda operação é executada do lado do datacenter, impedindo infecções e invasões, já que a máquina do usuário não tem conexão direta com o datacenter. Neste caso, a conexão sempre chegará segura ao lado do datacenter.

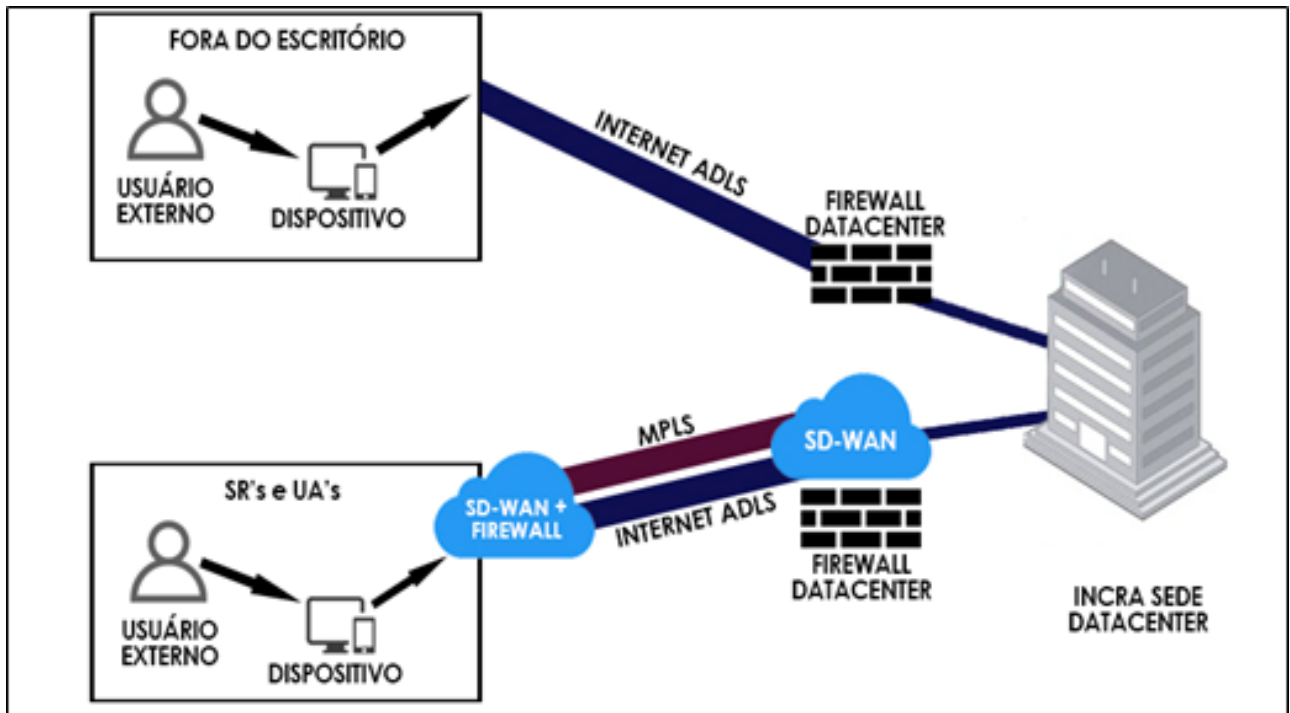


Figura 10: Topologia de Conexão de Acesso Seguro.

4.2.14.1. Para essa solução, os usuários acessarão um ambiente estruturado, "limpo" e padronizado, através de desktops ou aplicações virtuais, que estarão armazenadas e serão executadas no INCRA SEDE, sendo este responsável pela entrega desse modelo remoto aos colaboradores que precisam executar suas atividades fora do INCRA, e colaboradores internos. Os colaboradores também se beneficiarão de requisitos de segurança e proteção de dados, pois estes requisitos também estarão sob gestão da Sede e essa poderá aplicar controles de políticas conforme necessidade e demanda de segurança.

4.2.14.2. Com o uso desta solução, o INCRA se mantém aderente aos padrões nacionais de segurança de dados e busca entregar níveis excelentes de continuidade de negócio para seus colaboradores.

4.2.15. Para essa solução, algumas características se tornam extremamente necessárias para a operacionalização, alta experiência dos usuários e gestão:

CARACTERÍSTICA	CENÁRIO ATUAL	BENEFÍCIOS PROJETADO
Acesso remoto dos usuários	Acesso por meio de solução VPN, que propicia ou pode causar brechas de segurança e dificuldade de escala.	Permitir que os usuários realizem seu trabalho de qualquer lugar, estando preparado para o trabalho remoto.
Acesso remoto	Usuários que realizam acesso às aplicações do INCRA	Permitir que os usuários de unidades remotas utilizem de todas as

das SR's e UA's	que estão localizadas na SEDE enfrentam problemas de performance visto a dependência do link de conectividade, sendo apenas 1 link por local.	ferramentas que o INCRA possui, fazendo que realizem suas atividades diárias como se estivessem nas dependências da SEDE, com uma infraestrutura moderna e ágil, além da alta disponibilidade.
Suporte facilitado	Atualmente o INCRA possui ferramenta para abertura e registro de suporte de aos usuários, que é mantida pela empresa terceirizada atualmente sobre a gestão do contrato. Com a solução de espaço de trabalho virtual essa funcionalidade será exigida e esperada, onde servirá como meio de suporte mais avançado e nativo à solução.	Os usuários receberão suporte de uma forma ainda mais otimizada, através da solução de espaço de trabalho virtual, no qual este suporte será ocorrerá em tempo real com a facilidade proveniente da solução, permitindo que os usuários não percam tempo com suporte demorado, aumentando sua produtividade e tempo de uso das aplicações dentro dos limites legais de pessoal.
Melhoria de experiência	Cada aplicação é executada pelo usuário de forma segmentada, sempre exigindo a abertura de um navegador para acesso ou uma aplicação cliente-servidor, sem encontrar isso de forma centralizada.	Os usuários receberão um ambiente de trabalho organizado de acordo com sua necessidade e mais performático.
Acesso a partir de qualquer dispositivo	Os usuários acessam as aplicações e dados a partir de qualquer dispositivo, porém é inviável validar a segurança destes dispositivos e realizar controles avançados de ingresso e logon no ambiente, e com isso impossível de ser feito, brechas de segurança são abertas.	Os usuários iram acessar os aplicativos ou desktops virtuais por meio de canal seguro e terão seu acesso controlados, uma vez que será possível analisar o dispositivo do usuário e ainda ignorá-lo quando necessário, pois todas as ações que serão executadas no dispositivo do usuário não passam de comandos de tela, teclado e mouse criptografados enviados ao datacenter do INCRA, sendo assim o dispositivo do usuário deixa de ser um ponto de falha.

4.3. AGREGAÇÃO E BALANCEAMENTO DE LINKS.

4.3.1. Solução de agregação e balanceamento de links, para alta disponibilidade e conectividade avançada entre as unidades remotas e a sede, de acordo com as especificações do Anexo I – ETPC (10012570).

4.3.2. Justificativas.

4.3.2.1. A solução de conectividade de acesso permite que os colaboradores, quando acessarem diretamente das SR's e UA's, possam usufruir de uma conexão veloz e com alta disponibilidade.

4.3.2.2. A solução será a base de conectividade para os colaboradores das SR's, UA's e UAE's que hoje acessam especificamente por conexão única e não redundante de rede corporativa MPLS ou conexão comum de Internet.

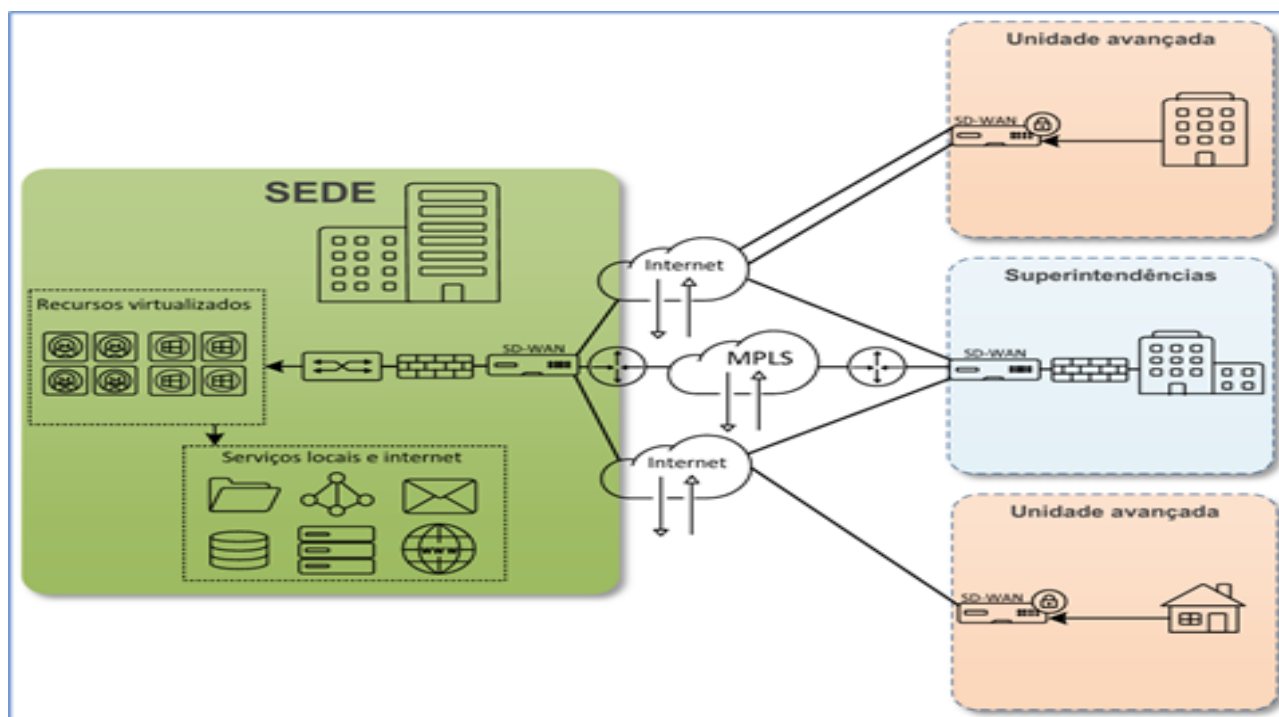


Figura 11: Modelo de conexão redundante de unidades remotas à Sede.

4.3.2.3. A solução de agregação e balanceamento permitirá a entrega de mais de um tipo de caminho de conexão para que os colaboradores possam realizar suas atividades sem a percepção de uma possível queda na rede de dados e seu trabalho não seja comprometido.

4.3.2.4. As unidades que já possuem rede MPLS, continuarão com essa conexão e será incluída outro tipo de conexão de internet do tipo Internet dedicada, de outra operadora, para que se aumente a disponibilidade e garanta a conexão de forma independente. Essa conexão será balanceada através de solução de *appliance* físico de conectividade de acesso, também conhecida como solução de SD-WAN, descrito neste projeto. Este *appliance* físico deverá receber 2 ou mais conexões de rede, permitindo que a tecnologia embarcada no *appliance* defina o melhor caminho de conexão no momento da transferência do pacote de dados, garantindo que a comunicação não seja interrompida mesmo no caso da falha de um dos links. Apenas do projeto inicialmente contar com o uso da atual rede MPLS para as unidades que já possuem essa conexão, instalando apenas mais um segundo link (fruto desta contratação), a solução será capaz de executar apenas com links de internet comuns ou dedicados, deixando de ser um requisito uma rede corporativa do tipo MPLS, reduzindo os custos de uso de uma rede MPLS se for o caso.

4.3.2.5. A entrega dos links à *appliance* do SD-WAN será feita da seguinte forma: a operadora de links de internet (no caso do atual MPLS, a CLARO/EMBRATEL - Processo volume II SEI nº 0115397 página 206), como complemento ao fornecimento de seu serviço de conectividade, um equipamento de rede (switch/roteador ou que for necessário) **que será utilizado em modelo de comodato**. Esse equipamento, é responsável por receber a conexão do link. O SD-WAN por sua vez, se conectará neste equipamento fornecido pela operadora de internet, para poder realizar a criação do "túnel virtual" que utilizará os dois caminhos de conexão para este fim.

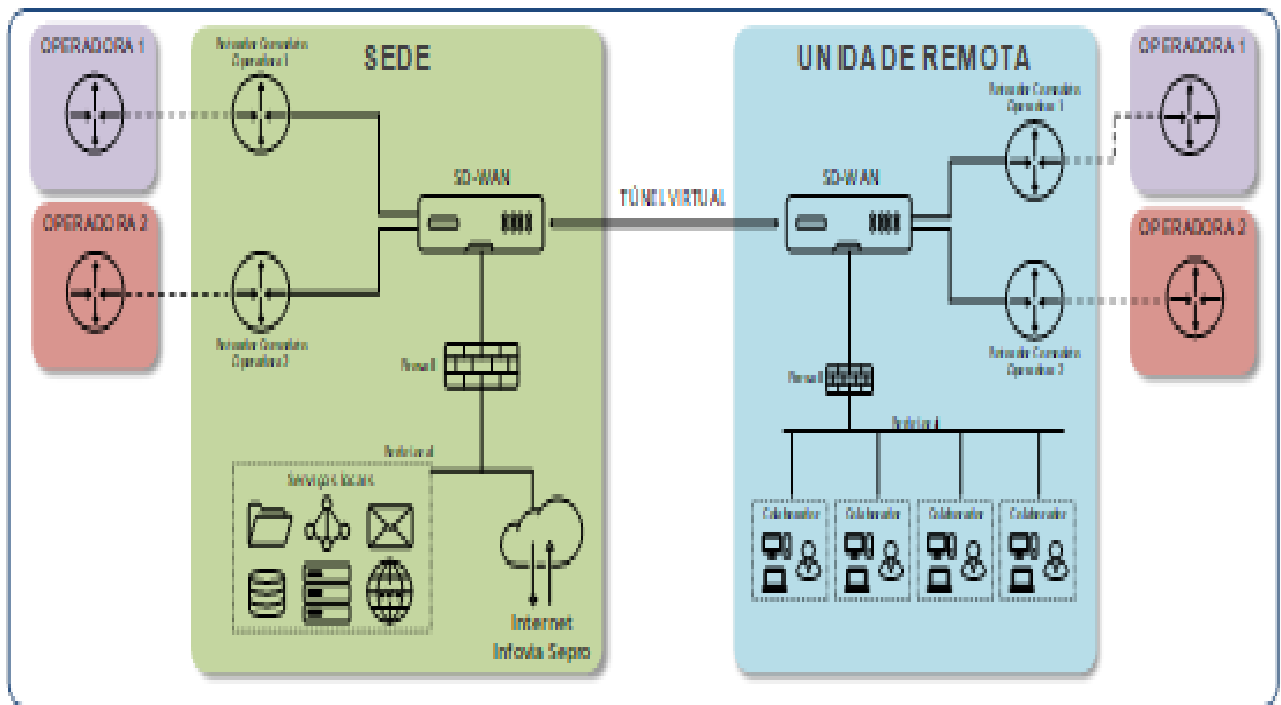


Figura 12: Conexão dos links de internet com o SD-WAN.

4.3.2.6. Com a solução proposta, as unidades remotas se conectarão diretamente à Sede, fazendo com que todas as unidades remotas possuam independência de conexão para uso de domínio único, portal de trabalho virtual, dados, etc. Com isso o INCRA adquire benefícios de gestão e suporte sobre as unidades remotas avançadas que outrora não se possuía tal gestão ou visibilidade sobre elas e que poderá gerar, inclusive, economia na aquisição de ativos de rede.

4.3.2.7. A solução criará um caminho virtual único, se utilizando dos dois links apresentados, sempre escolhendo o melhor caminho disponível e ainda realizando a alta disponibilidade de conexão. Esse caminho virtual será criptografado e seguro, sendo usado apenas para comunicação de uma unidade remota ao INCRA Sede.

4.3.2.8. A *appliance* de conectividade possui papel extremamente importante para a entrega eficiente e altamente disponível dos links de conexão. Além de seus recursos avançados de alta disponibilidade de conexão e conectividade de unidades remotas, a solução entregará outras características, tais como segurança, otimização e roteamento de redes. Isso se torna um requisito pois algumas SR's e UA's não possuem infraestrutura de datacenter, rede e segurança, e tal *appliance* física atenderá às demandas dessas localidades.

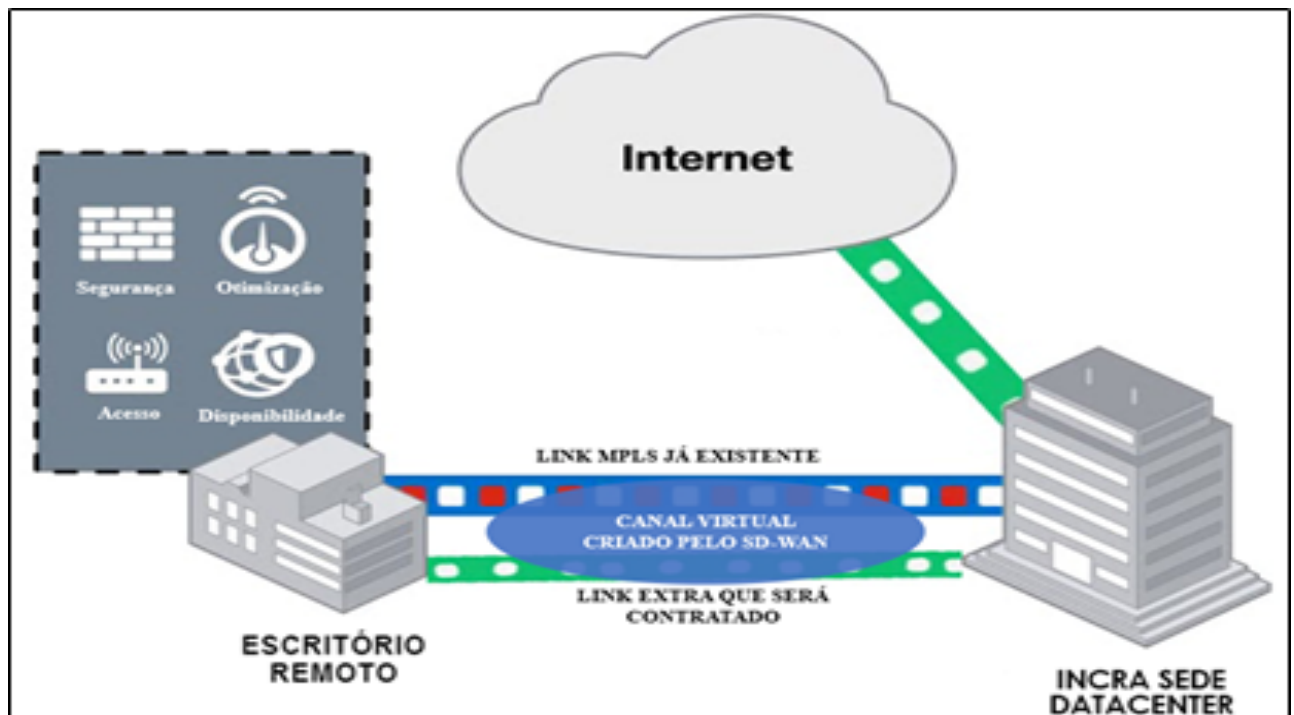


Figura 13: Funcionalidades SD-WAN.

4.3.2.9. Vale lembrar que essa solução beneficiará os colaboradores quando utilizando a infraestrutura dos escritórios remotos (SR's e UA's), pois haverá uma *appliance* em cada unidade remota criando o link virtual com a SEDE, onde estarão localizadas as aplicações e dados após a centralização. Quando o usuário estiver externamente, ou seja, fora dos escritórios remotos, ele utilizará sua conexão própria de internet, mas ainda assim se beneficiando dos itens explanados na solução de espaço de trabalho virtual.

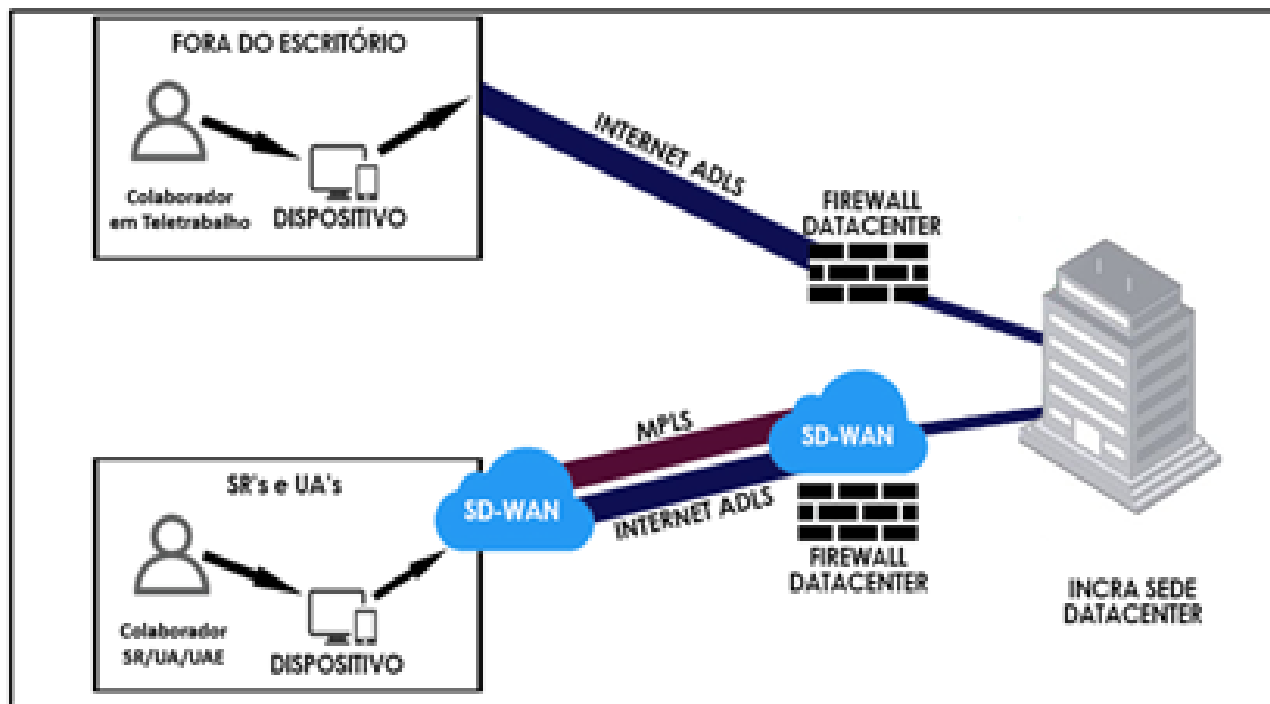


Figura 14: Topologia de Conexão de Acesso Otimizado (SD-WAN).

4.3.2.10. A solução também irá permitir que as unidades remotas possam acessar à internet localmente, também com alta disponibilidade, sem a necessidade de que todo o fluxo de dados para saída à internet seja direcionado para o INCRA Sede. Esse acesso poderá ser feito local e tratado com segurança e confiabilidade.

4.3.2.11. Vale lembrar, que a contratação destes serviços também vai ao encontro das diretrizes do Governo Federal, especialmente pelas normas e recomendações emitidas pela Secretaria de Governo Digital (SGD) do Ministério da Economia, órgão central do Sistema de Administração dos Recursos de Tecnologia da Informação – SISIP, além de atender aos requisitos de Estratégia de Governança Digital do Governo Federal.

4.3.2.12. Quando é realizado um comparativo exemplificativo da solução de conectividade entre as unidades utilizando o SD-WAN frente à conectividade com a atual rede MPLS, pode-se identificar como as principais diferenças aquelas apresentadas abaixo:

CARACTERÍSTICA	MPLS	SD-WAN
Opções de conectividade	Apenas rede MPLS	Combinação de rede MPLS, Internet e 4G
Opções de acesso à Internet pelas unidades remotas	Tráfego retorna para o Datacenter e de lá para a Internet	Opção de acesso diretamente pela localidade
Escalabilidade	Requer longa negociação com a operadora para aumento de capacidade	Opção de inclusão de capacidade pela contratação de outro link banda larga mais barato
Qualidade	Baixa	Alta
Segurança	Baixa – O tráfego precisa retornar ao datacenter para ser inspecionado	Alta – Segurança embarcada e segmentação de rede
Visibilidade de conexões/aplicações	Baixa	Alta e profunda visibilidade
Alcance geográfico	Limitado à capacidade da operadora	Limitado à latência suportada pelas aplicações (sem limitação física)
Impacto de custo	Altos custos	Baixo – Uma vez que podem ser utilizados links comuns
Gerenciamento	Descentralizado	Centralizado
Alta disponibilidade	Não existe	Completamente configurado, pois pode-se utilizar vários links

4.3.2.13. Com a resolução da problemática de acesso sem alta disponibilidade, o INCRA será capaz de unificar seus datacenters e manter toda a estrutura de dados e aplicações centralizadas no INCRA Sede, atendendo como provedor de serviços de TI à todas as unidades remotas com os altos níveis esperados de entrega de serviço.

4.3.2.14. Diante os dados expostos, citam-se como pontos primordiais da solução de SD-WAN, os seguintes:

- **Conectividade:** extensão da rede local do INCRA entre suas unidades, permitindo que os colaboradores utilizem o domínio único, as aplicações e dados localizados no INCRA Sede como se fisicamente estivessem neste local;
- **Experiência:** uma vez que o SD-WAN pode receber a conectividade de vários links, a banda de conexão pode ser facilmente aumentada para prover maior performance aos usuários;
- **Segurança:** SD-WAN utilizará segurança embarcada para a proteção dos acessos à Internet de forma otimizada, e sem a necessidade de retornar todos os tráfegos, até quando não são necessários, para o Datacenter do INCRA, liberando essa conexão para os fins que forem necessários.
- **Gerenciamento:** SD-WAN será gerido por um local único, sem a necessidade de ações descentralizadas e repetitivas;
- **Visibilidade:** SD-WAN será a entidade responsável por gerir o nível de qualidade entregue pelos links contratados. Além disso, o SD-WAN proverá visibilidade ponta-a-ponta para as conexões dos usuários, e com isso permitirá uma melhor e mais rápida resolução de problemas.

4.3.2.15. Para essa solução, algumas características se tornam extremamente necessárias para a operacionalização e gestão da plataforma:

CARACTERÍSTICA	CENÁRIO ATUAL	BENEFÍCIOS
Disponibilidade de conexão	O acesso é realizado pelos colaboradores através de um link único já existente (MPLS ou INTERNET) onde as conexões às	O acesso dos colaboradores, quando executado de dentro das unidades remotas do INCRA estará totalmente disponível visto a tecnologia de agregação e balanceamento da conexão (SD-WAN), onde essa fará, de forma inteligente, a

	aplicações instaladas no INCRA SEDE, ficam reféns da disponibilidade dessa conexão, sendo isso um ponto crítico de falha e de performance aos colaboradores.	escola da melhor conexão, sendo link Internet (previsto neste projeto) ou link atualmente instalado nas unidades (MPLS ou Internet).
Segurança de conexão de rede	A segurança das unidades remotas é uma atribuição do INCRA Sede, o qual tem o papel de receber todos os acessos à internet realizados pelas unidades remotas e tratá-los em requisitos de segurança e controle de dados.	Os acessos poderão ser tratados localmente nas unidades remotas, uma vez que a solução permitirá que, quando se tratar de sítios na internet, esse tráfego de rede não seja direcionado para o INCRA Sede, sendo enviado através da solução diretamente pela internet, porém aplicando níveis de segurança de acesso.
Centralização de dados e aplicações	Cada unidade possui seu datacenter instalado localmente para suportar suas aplicações locais e dados, isso se torna com o passar do tempo caro de difícil administração.	O INCRA Sede realizará a entrega de todas as aplicações, sendo assim, os colaboradores acessarão suas aplicações a partir de um portal onde receberão de forma virtualizada esses recursos, obtendo uma melhora na experiência e um ambiente seguro, controlado e organizado com tudo necessário para sua atividade. Não será necessário que cada unidade remota construa e mantenha seu datacenter para suporte às suas aplicações, desonerando financeiramente e tecnologicamente estas unidades.

Tabela de características e recursos 2

4.4. LINK DE INTERNET

4.4.1. Fornecimento de link de Internet redundante para localidades remotas do INCRA (SR's, UA's e UAE's).

4.4.2. Justificativas

4.4.2.1. A necessidade aquisição de prestação de serviços para fornecimento de link de internet redundante foi amplamente embasado conforme necessidades dos demais itens previamente citados.

4.4.2.2. A aquisição deste link redundante se dará da seguinte forma:

- Entrega de links de Internet redundante (dois links) dedicada para cada unidade remota do tipo SR e aquelas UA's equivalentes a SR, entregando esta conexão por provedores diferentes ou meios físicos diferentes (Roteadores, Backbones e etc), buscando garantir a alta disponibilidade, ou seja, ao menos um link deve sempre estar disponível caso o outro falhe. Os links redundantes são contemplados nos itens 1 e 2 do Grupo 3.
- Para as Superintendências Regionais (SR's) devem ser entregues links através de conexão de fibra ótica, para as demais localidades (UA's e UAE's) podem ser utilizados outros meios de entrega quando a fibra ótica não estiver disponível.
- O INCRA contratará dois links de Internet redundante com a velocidade de 20Mbps, porém, o INCRA prevê a inclusão de velocidade para cada link, com isso a CONTRATADA deve sempre garantir que todos os links, em todas as localidades, devem possuir escalabilidade de até 40Mbps (o dobro da velocidade).

4.4.2.3. A aquisição de links é necessária para atingir os benefícios esperados da tecnologia de agregação e balanceamento de links aplicada, que necessita de um meio físico a ser transmitido os dados entre as localidades. Neste caso a solução se beneficiará da malha de internet para "enxergar" as unidades remotas através da Sede, fazendo com que assim seja criado uma rede virtual estendida e única do INCRA, espalhada por todo o Brasil.

4.4.2.4. Para este item não há a necessidade de aquisição conectividade corporativa dedicada, podendo a solução trafegar sob redes mais baratas e de maior simplicidade de operação.

4.4.2.5. Para essa solução, algumas características se tornam extremamente necessárias para a operacionalização e gestão da plataforma:

CARACTERÍSTICA	CENÁRIO ATUAL	BENEFÍCIOS
Inclusão de caminho extra de acesso	Sem caminho redundante de conexão, visto a utilização de apenas um link de conexão entre as unidades.	Um segundo link de conexão à internet será utilizado para conectar as unidades remotas à Sede através de protocolos seguros.

Tabela de características e recursos 3

4.5. SERVIÇOS RELACIONADOS ÀS SOLUÇÕES E EQUIPAMENTOS A SEREM ADQUIRIDOS.

4.5.1. Todos as soluções contratadas deverão contar com os seguintes serviços de acordo com as especificações do Anexo I - ETPC(10012570):

4.5.1.1. Garantia técnica durante o período de 12 meses, renováveis até 60, a contar da Emissão do Termo de Recebimento Definitivo - TRD, e subsequente Nota Fiscal dos equipamentos/serviços;

4.5.1.2. Suporte técnico oficial 24 horas por dia e 7 dias por semana, inclusive feriados;

4.5.1.3. Instalação e Configuração;

4.5.1.4. Repasse de Conhecimento;

4.5.1.5. Treinamento.

5. ANÁLISE COMPARATIVA DAS SOLUÇÕES (IN SGD/ME Nº 01/2019, ART.11, INCISO I)

5.1. O mercado de soluções para soluções de espaço de trabalho virtual mostra-se altamente concentrado, por se tratar de soluções exclusivas e altamente características, mas há diversos fornecedores disponíveis. Isso garante a competitividade de um processo licitatório, conforme verifica-se no estudo de quadrantes elaborado pela consultoria IDC, referente ao ano de 2019.

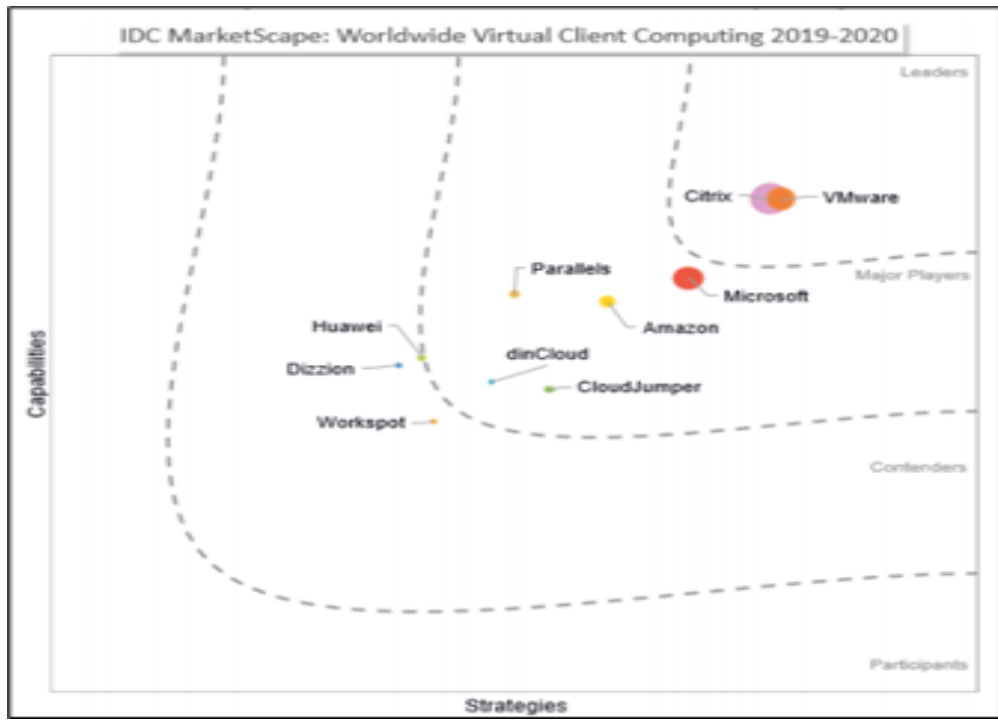


Figura 15: IDC MarketScape “Worldwide Virtual Client Computing 2019–2020 Vendor Assessment” (04/2020).

5.2. O mercado de soluções de SD-WAN mostra-se altamente concentrado, por se tratar de soluções exclusivas e altamente características, mas há diversos fornecedores disponíveis. Isso garante a competitividade de um processo licitatório, conforme verifica-se no estudo de quadrantes elaborado pelo Gartner, referente ao ano de 2019.



Figura 16: Quadrante mágico Gartner “Magic Quadrant for WAN Edge Infrastructure” (09/2020)

5.3. Identificação e Análise Comparativas das Soluções de TIC no mercado:

5.3.1. SOLUÇÃO DE ESPAÇO DE TRABALHO VIRTUAL

5.3.1.1. Identificação das soluções de TIC disponíveis no mercado:

ID SOLUÇÃO	DESCRIÇÃO RESUMIDA	DESCRIÇÃO BREVE
1	Aquisição de Espaço de Trabalho Virtual	<p>São sistemas virtuais que entregam um portal seguro ao usuário, unificando aplicações (de qualquer tipo e versão), desktops virtuais e dados centralizados e organizados de forma simples, contemplando também ferramentas de controle de segurança e sem a necessidade de gerir a máquina do usuário final, que pode ser qualquer tipo de dispositivo. São soluções de espaço de trabalho virtual:</p> <ul style="list-style-type: none"> • Citrix Virtual Apps and Desktops • Citrix Workspace • VMware Horizon • VMware Workspace One

2	Expansão de Solução de VPN (Virtual Private Access) para acesso remoto.	São soluções tradicionais de acesso remoto, porém sem controles de segurança avançados, trazendo riscos adicionais de conectividade às aplicações e dados.
---	---	--

Tabela com as tecnologias disponíveis no mercado compatíveis com os requisitos técnicos.

5.3.1.2. Soluções similares em outros órgãos:

ORGÃOS PÚBLICOS QUE CONTRATARAM SOLUÇÃO DE ESPAÇO DE TRABALHO VIRTUAL	
BANCO DE BRASÍLIA SA - BRB	
Descrição do Objeto Contratado	Aquisição de Software de virtualização de desktops para suporte ao ambiente de VDI
Valor da Contratação	R\$ 8.990.000,00
Processo Licitatório	64/2019
TRIBUNAL SUPERIOR DO TRABALHO	
Descrição do Objeto Contratado	Suporte técnico para a plataforma de produtos Citrix XenDesktop Enterprise Edition e subscrições com direito a atualização de versão das licenças Citrix XenDesktop.
Valor da Contratação	R\$ 597.600,00
Processo Licitatório	113/2017
TRIBUNAL DE JUSTIÇA DE SANTA CATARINA	
Descrição do Objeto Contratado	VMware Horizon Standard, licenciamento concorrente, suporte de 60 meses
Valor da Contratação	R\$ 1.727.598,00
Processo Licitatório	170/2017
CONTROLADORIA GERAL DA UNIÃO	
Descrição do Objeto Contratado	Licenciamento perpétuo de solução de virtualização de desktops, com suporte técnico e direito de atualização por 36 meses.
Valor da Contratação	R\$ 2.548.000,00
Processo Licitatório	17/2020
AGÊNCIA NACIONAL DE ENERGIA ELÉTRICA	
Descrição do Objeto Contratado	Licenças de software de virtualização (licenciamento perpétuo) e gerenciamento do ambiente de virtualização de desktops, incluindo instalação, suporte técnico e garantia pelo prazo de 60 meses.
Valor da Contratação	R\$ 3.430.200,00
Processo Licitatório	26/2020

Tabela de soluções de espaço de trabalho virtual no poder público.

- Através da necessidade dos órgãos governamentais de centralizarem seus datacenters e conseqüentemente suas aplicações e dados, surge a necessidade de uso de solução que permita e facilite acesso dos colaboradores aos ativos centralizados. Ocorrendo isso, torna-se necessário a aquisição de soluções de espaço de trabalho virtual a fim de garantir a correta entrega dos serviços e atendimento aos níveis adequados de serviço, além de garantir ainda, a segurança dos dados.
- As soluções de acesso remoto através de espaço de trabalho virtual estão amplamente sendo utilizadas nas instituições públicas do Brasil, pois se tornou um modelo de entrega virtual completamente customizado, tornando aderente a qualquer necessidade dos órgãos.
- Em relação ao ID SOLUÇÃO 2 (Expansão de VPN), diversos órgãos da administração pública utilizam esta solução para permitir que determinados colaboradores acessem a sua estrutura tecnológica. Entretanto esse tipo de acesso deve ser controlado, sendo realizado por servidores pontuais (da área de TI) e através de dispositivos corporativos completamente atualizados, a fim de mitigar problemas de segurança através desses acessos. Desta forma, não são soluções excludentes, sendo passíveis de funcionamento em paralelo, cada qual em sua determinada e específica função para a qual fora desenvolvida.

5.3.1.3. Tabela comparativa conforme observações do inciso II do artigo 11 da IN 01 SGD/ME 2019

ID SOLUÇÃO	Disponibilidade de solução similar em outro órgão	Política, os modelos e os padrões de governo	Necessidade de adequação do ambiente do órgão	Contratação como serviço	Diferentes modelos de prestação de serviço e tipos de soluções
1	Sim, conforme item 5.3.1.2	Aderente por padrão	Não	Não há exemplo similar na administração pública	Sim
2	Sim, conforme item 5.3.1.2	Aderente por padrão	Não	Não há exemplo similar na administração pública	Sim

Tabela de Conformidade com a IN SGD/ME 01/2019

5.3.2. SOLUÇÃO DE AGREGAÇÃO E BALANCEAMENTO DE LINKS

5.3.2.1. Identificação das soluções de TIC disponíveis no mercado:

ID SOLUÇÃO	DESCRIÇÃO RESUMIDA	DESCRIÇÃO BREVE
1	Aquisição de Solução para Agregação e Balanceamento da Conexão de Acesso para SR's e UA's com Link Redundante.	É uma solução que permite a otimização e alta disponibilidade da conexão dos usuários de unidades remotas à unidade central (datacenter), incluindo funcionalidades para facilitar a integração nas unidades.
2	Aquisição de Link MPLS extra sem alta disponibilidade para as localidades remotas.	É um modelo de aquisição de um caminho de conectividade extra para as unidades remotas do INCRA, sendo necessário que este link seja um novo link MPLS (preferencialmente de outra operadora), ou um link de Internet dedicada, sendo que nesta segunda opção é necessário que outros equipamentos façam o papel de conectar as unidades remotas à Sede através do link de internet.
3	Aquisição de Link extra com alta disponibilidade via solução de software livre.	É um modelo similar à solução de ID 2, onde adição é utilizado um componente de software, baseado em software livre, para uso que este faça a ação de chaveamento de conectividade entre os links, para que em caso de queda de qualquer um dos links, a solução faça a transferência de todos os acessos para o segundo link disponível.

Tabela 7: Tabela com as tecnologias disponíveis no mercado compatíveis com os requisitos técnicos

5.3.2.2. Soluções similares em outros órgãos:

ORGÃOS PÚBLICOS QUE CONTRATARAM SOLUÇÃO DE AGREGAÇÃO E BALANCEAMENTO	
BANCO DO NORDESTE	
Descrição do Objeto Contratado	Serviço de Rede WAN Definida por Software
Valor da Contratação	R\$ 9.478.719,84
Processo Licitatório	2018/044 - https://www.bnb.gov.br/aplicacao/fornecedores/Editais_Publicados/Editais/EDT_PE_2018_044_nova%20versao.pdf
ANAC – AGÊNCIA NACIONAL DE AVIAÇÃO CÍVIL	
Descrição do Objeto Contratado	Otimização de link e virtualização de serviços e de rede WAN
Valor da Contratação	R\$ 6.925.230,00
Processo Licitatório	37/2020 https://www.gov.br/anac/pt-br/aceso-a-informacao/licitacoes-e-contratos/licitacoes-2020/pregao-37-2020/pregao-37_2020-aquisicao-de-equipamento-de-sdwan-srp_comprasnet.pdf

Tabela de Soluções de conectividade de acesso.

5.3.2.3. Tabela comparativa conforme observações do inciso II do artigo 11 da IN 01 SGD/ME 2019.

ID SOLUÇÃO	Disponibilidade de solução similar em outro órgão	Política, os modelos e os padrões de governo	Necessidade de adequação do ambiente do órgão	Contratação como serviço	Diferentes modelos de prestação de serviço e tipos de soluções
1	Sim, conforme item 5.3.2.2	Aderente por padrão	Não	Não há exemplo similar na administração pública	Sim
2	Sim, conforme item 5.3.2.2	Aderente por padrão	Não	Não há exemplo similar na administração pública	Sim
3	Sim, conforme item 5.3.2.2	Aderente por padrão	Não	Não há exemplo similar na administração pública	Sim

Tabela de Conformidade com a IN SGD/ME 01/2019.

5.3.3. SERVIÇO DE LINK DE INTERNET

5.3.3.1. Identificação das soluções de TIC disponíveis no mercado:

ID SOLUÇÃO	DESCRIÇÃO RESUMIDA	DESCRIÇÃO BREVE
1	Aquisição de Link de Internet Adicional	Será adquirido serviço de fornecimento de um link de internet extra para cada localidade remota (SR e UA).

Tabela com as tecnologias disponíveis no mercado compatíveis com os requisitos técnicos.

5.3.3.2. Soluções similares em outros órgãos:

ORGÃOS PÚBLICOS QUE CONTRATARAM SOLUÇÃO DE CONECTIVIDADE DE ACESSO	
PREFEITURA DA ESTÂNCIA BALNEÁRIOD DA PRAIA GRANDE	
Descrição do Objeto Contratado	Contratação de Empresa Especializada para Prestação de Serviço de Fornecimento de 02 (dois) Links Dedicados para Acesso à Internet.
Valor da Contratação	-
Processo Licitatório	089/2018 - https://www.praia grande.sp.gov.br/arquivos/pregao/18989.pdf
EMPRESA DE ASSISTÊNCIA TÉCNICA E EXTENSÃO RURAL – EMATER-DF	
Descrição do Objeto Contratado	Serviço de Comunicação de Dados para conexão da rede da EMATER-DF Sede à internet, por meio de link dedicado.
Valor da Contratação	-
Processo Licitatório	019/2017 https://emater.df.gov.br/wp-content/uploads/2018/04/Edital-Aquisi%3%a7%3%a3o-de-Link-Internet-164.2017.pdf

Tabela de Soluções de link de internet.

5.3.3.3. Tabela comparativa conforme observações do inciso II do artigo 11 da IN 01 SGD/ME 2019.

ID SOLUÇÃO	Disponibilidade de solução similar em outro órgão	Política, os modelos e os padrões de governo	Necessidade de adequação do ambiente do órgão	Contratação como serviço	Diferentes modelos de prestação de serviço e tipos de soluções
1	Sim, conforme item 5.3.2.2	Aderente por padrão	Não	Sim	Sim

Tabela de Conformidade com a IN SGD/ME 01/2019.

5.3.4. SERVIÇOS RELACIONADOS AOS ITENS A SEREM ADQUIRIDOS

5.3.4.1. Identificação das soluções de TIC disponíveis no mercado:

- Os ativos de TI devem ser adquiridos com garantia de funcionamento provida pelo fornecedor durante sua vida útil, salvo quando justificado o contrário e com relação ao ativo em específico.
- Os serviços são de Repasse de Conhecimento; Instalação e Configuração; Garantia técnica durante **12 meses (renováveis até 60)**; Suporte técnico oficial 24 horas por dia e 7 dias por semana, inclusive feriados; e contemplar treinamento. São serviços essenciais ao pleno funcionamento dos equipamentos que serão adquiridos, tanto para implantação quanto para continuidade do negócio.

5.3.4.2. **Soluções similares em outros órgãos:**

- As mesmas citadas nos itens 5.3.1.2 e 5.3.2.2 pois se trata de serviços referente aos itens já citados.

5.3.4.3. **Tabela comparativa conforme observações do inciso II do artigo 11 da IN 01 SGD/ME 2019.**

- Estes serviços relacionados são padronizados e muito similares.

ID SOLUÇÃO	Disponibilidade de solução similar em outro órgão	Política, os modelos e os padrões de governo	Necessidade de adequação do ambiente do órgão	Contratação como serviço	Diferentes modelos de prestação de serviço e tipos de soluções
1	Sim, conforme item 5.3.2.2	Aderente por padrão	Não	Não há exemplo similar na administração pública	Sim

5.3.5. **COMUM A TODOS OS ITENS E GRUPOS.**5.3.5.1. **Requisitos IN 01/2019 - art. 11, III (será o mesmo para todos) e para pleno funcionamento das soluções a serem adquiridas.**

REQUISITO IN SGD/ME 01/2019	ID SOLUÇÃO POR ITEM	SIM	NÃO	NÃO SE APLICA
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	ESPAÇO DE TRABALHO VIRTUAL (1 e 2)		X	
A Solução é composta por software livre ou software público? (quando se tratar de software)			X	
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	AGREGAÇÃO E BALANCEAMENTO DE LINKS (1, 2 e 3)			X
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	LINK DE INTERNET (1)			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	SERVIÇOS RELACIONADOS (1)			X

Tabela de Requisitos da IN SGD/ME 01/2019 - <https://www.gov.br/governodigital/pt-br/contratacoes/templates-e-listas-de-verificacao>

- **Soluções existentes no Portal do Software Público Brasileiro ou software livre**

*Não se aplica, visto se tratar de solução de tecnologia da informação. Todavia, apesar de necessitar de software para a operação, não foram encontradas soluções livres que atendam a tal requisito.

- **Aderência aos padrões e-Ping, e-Mag e e-Pwg**

*Considerando que a iniciativa não trata de interoperabilidade entre sistemas ou organizações ou trata de acessibilidade digital, este item não se aplica.

- **Aderência às regulamentações da ICP-Brasil**

*Considerando que a iniciativa não trata de certificados digitais, este item não se aplica.

- **Aderência ao e-ARQ Brasil**

*Considerando que a iniciativa não trata de sistemas informatizados de Gestão Arquivística de Documentos, este item não se aplica.

5.3.5.2. **Recursos materiais e humanos para pleno funcionamento das soluções a serem adquiridas.**

- Os recursos materiais e humanos necessários para viabilização da execução contratual no ambiente do órgão, exemplo: mobiliário, instalação elétrica, espaço adequado para prestação do serviço, etc., estão discriminados abaixo e poderão ser verificados quando da visita técnica necessária na etapa do processo licitatório:

RECURSOS MATERIAIS PARA SUSTENTAR A CONTRATAÇÃO						
ID SOLUÇÃO POR ITEM	IMPACTO	RECURSO	QUANTIDADE NECESSÁRIA	DISPONIBILIDADE	AÇÃO	RESPONSÁVEL
ESPAÇO DE TRABALHO VIRTUAL (1 e 2)	NENHUM, POIS JÁ SE TRATA DE UM SERVIÇO QUE ESTÁ SENDO CONTEMPLADO NO PROJETO, POR ISSO, TORNA-SE ATENDIDO.	Link de internet para as unidades remotas (SR's e UA's) do INCRA.	Mensurado de acordo com as quantidades de unidades remotas atuais.	Integral	Verificar os requisitos necessários para instalação dos links em cada localidade.	INCRA/DO/DOT
AGREGAÇÃO E BALANCEAMENTO DE LINKS (1, 2 e 3)						
LINK DE INTERNET (1)	NENHUM, POIS JÁ SE TRATA DE UM SERVIÇO JÁ IMPLEMENTADO.	Rede lógica	Mensurado de acordo com os equipamentos já em produção nas unidades remotas.	Integral	Verificar se a rede lógica está em pleno funcionamento.	INCRA/DO/DOT
SERVIÇOS RELACIONADOS (1)						

Tabela de Recursos Materiais

RECURSOS HUMANOS NECESSÁRIOS PARA SUSTENTAR A CONTRATAÇÃO	
Atribuições Gestor do Contrato	Servidor com capacidade gerencial, técnica e operacional relacionada ao processo de gestão do contrato, indicado pela autoridade competente da área de TI.
Fiscal Técnico (Titular e Suplente)	Servidor da Área de Tecnologia da Informação, indicado pela autoridade máxima dessa área.
Fiscal Administrativo (Titular e Suplente)	Servidor da área administrativa, indicado pela autoridade máxima dessa área.

Fiscal Requisitante (Titular e Suplente)	Servidor da Área Requisitante da Solução, indicado pela autoridade máxima dessa área.
Preposto da Contratada	Interlocutor da empresa prestadora do serviço com o INCR.

Tabela de Recursos Humanos

5.3.6. MODALIDADE DE LICITAÇÃO

5.3.6.1. Acredita-se que seja o caso de aplicação do Decreto nº 10.024, de 20 de setembro de 2019 que regulamenta a licitação, na modalidade pregão, na forma eletrônica, para a aquisição de bens e a contratação de serviços comuns, incluídos os serviços comuns de engenharia, e dispõe sobre o uso da dispensa eletrônica, no âmbito da administração pública federal, por ser a forma mais adequada para efetivação desta contratação, haja vista que trata-se de bens ou serviços considerados comuns na área de tecnologia da informação e comunicação. Ademais, o seu fornecimento obedece a padrões pré-estabelecidos e como são facilmente encontrados no mercado e fornecido por diversas empresas; e deve-se considerar, também, que é uma forma célere de contratação.

"Art. 1º Este Decreto regulamenta a licitação, na modalidade de pregão, na forma eletrônica, para a aquisição de bens e a contratação de serviços comuns, incluídos os serviços comuns de engenharia, e dispõe sobre o uso da dispensa eletrônica, no âmbito da administração pública federal." (GRIFO NOSSO)

5.3.7. SEPARAÇÃO DOS ITENS DA CONTRATAÇÃO EM GRUPOS E ITENS

5.3.7.1. Para esta contratação haverá separação em Grupos com itens específicos para cada um, sendo três grupos no total. Três grupos foram criados, por entender que a competitividade de mercado e a ampla concorrência seriam beneficiados. O grupo 3, por sua importância, é tratado com um serviço específico, sendo assim, o INCR define que os vencedores dos grupos 1 e 2, não poderão ser os mesmos vencedores do grupo 3. Essa imposição se dá ao fato de que a(s) empresa(s) vencedora(s) do grupo 1 e/ou 2, através de suas soluções, entregarão informações técnicas durante o contrato que permitirão a fiscalização e controle sobre os níveis de qualidade aceitável sobre os links entregues. Sendo assim, para garantir a qualidade e isonomia nos levantamentos técnicos e fiscalização, as empresas deverão ser distintas.

5.3.7.2. A fim de esclarecer as possibilidades de vencimento dos grupos por empresas participantes, segue simulações de cenários POSSÍVEIS e IMPOSSÍVEIS de homologação:

SIMULAÇÃO POSSÍVEL 1 – VENCEDORES DIFERENTES PARA CADA GRUPO	
GRUPO 1	Vencedora EMPRESA A
GRUPO 2	Vencedora EMPRESA B
GRUPO 3	Vencedora EMPRESA C
SIMULAÇÃO POSSÍVEL 2 – MESMOS VENCEDOR PARA GRUPO 1 E 2	
GRUPO 1	Vencedora EMPRESA A
GRUPO 2	Vencedora EMPRESA A
GRUPO 3	Vencedora EMPRESA C
SIMULAÇÃO IMPOSSÍVEL 1 – MESMOS VENCEDOR PARA GRUPO 1 E 3	
GRUPO 1	Vencedora EMPRESA C
GRUPO 2	Vencedora EMPRESA A
GRUPO 3	Vencedora EMPRESA C
SIMULAÇÃO IMPOSSÍVEL 2 – MESMOS VENCEDOR PARA GRUPO 2 E 3	
GRUPO 1	Vencedora EMPRESA A
GRUPO 2	Vencedora EMPRESA C
GRUPO 3	Vencedora EMPRESA C

Tabela de cenários de homologação dos grupos

5.3.8. VIGÊNCIA CONTRATUAL DE CADA GRUPO

5.3.8.1. A Equipe de Planejamento da Contratação em conjunto com Coordenação Geral de Tecnologia e Gestão da Informação - DOT, acreditam que a previsão de vigência contratual para todos os grupos com base na Lei nº 8.666/1993 que dispõe sobre a regra, em tese, da vigência contratual em 12 meses.

5.3.8.2. Considerando ainda o Anexo IX da IN SEGES/MP nº 05/2017 que dispõe sobre as regras e diretrizes do procedimento de contratação de serviços sob o regime de execução indireta no âmbito da Administração Pública federal direta, autárquica e fundacional, *in verbis*:

"Anexo IX

12. Nos contratos de prestação de serviços de natureza continuada, deve-se observar que:

a) o prazo de vigência originário, de regra, é de 12 (doze) meses;

b) excepcionalmente, este prazo poderá ser fixado por período superior a 12 meses, nos casos em que, diante da peculiaridade e/ou complexidade do objeto, fique tecnicamente demonstrado o benefício advindo para a Administração; e

c) é juridicamente possível a prorrogação do Contrato por prazo diverso do contratado originalmente." (GRIFO NOSSO)

5.3.8.3. Ademais, deve-se considerar que para minimizar os riscos de gestão das licenças e volumetria contratada, a revisão anual é uma iniciativa que se apresentar atrativa para APF, pois poderá renegociar o quantitativos e valores dos itens a cada renovação contratual.

5.3.8.4. Ante ao exposto, o ideal, em tese, é que a **vigência contratual para todos os grupos seja de 12 meses renováveis por 48 meses, a fim de completar 60 meses ao final de contrato, que já contempla o período de garantia e todos os seus desembolsos anuais**, junto à prestação de serviço de Suporte 24x7 da solução.

5.3.9. ANÁLISE SOBRE OS ASPECTOS QUE ENVOLVEM A GARANTIA COM SUPORTE TÉCNICO EMBUTIDO

5.3.9.1. Inicialmente é importante ressaltar que nos processos de aquisições de bens de Tecnologia da Informação - TI, devido às suas características técnicas e por serem investimentos de alto custo, será sempre necessário que esses bens sejam acompanhados de uma garantia e de suporte para fins de assegurar o perfeito funcionamento da solução, como previsto no documento "Orientações para elaboração / ajuste de especificações técnicas de ativos de TI – Versão 4.0", vinculado à Portaria nº 20 de 14 de julho de 2016 da Secretaria de Tecnologia da Informação do Ministério do Planejamento – Portaria MP/STI nº 20/2016 – e ratificado pela Instrução Normativa nº 1, de 4 de abril de 2019.

5.3.9.2. Neste sentido, observa-se que no mercado a **garantia pode ser adquirida de forma embutida no valor total do bem** ou pode ser separada em um item exclusivo; isso ocorre, por exemplo, quando necessita-se da valorização de cada componente da solução, neste caso da garantia. Em ambos os casos, a garantia é item indissociável do bem, logo, sua contraprestação é na sua entrega, ocasionando a necessidade da justa liquidação financeira em conformidade com o subitem 1.2.1. das Orientações para elaboração / ajuste de especificações técnicas de ativos de TI – Versão 4.0 e pelo Art. 50, parágrafo único da Lei 8.078/1990.

"Art. 50. A garantia contratual é complementar à legal e será conferida mediante termo escrito.

Parágrafo único. O termo de garantia ou equivalente deve ser padronizado e esclarecer, de maneira adequada em que consiste a mesma garantia, bem

como a forma, o prazo e o lugar em que pode ser exercitada e os ônus a cargo do consumidor, **devendo ser-lhe entregue, devidamente preenchido pelo fornecedor, no ato do fornecimento, acompanhado de manual de instrução, de instalação e uso do produto em linguagem didática, com ilustrações.**" Lei nº 8.078/1990 (GRIFO NOSSO)

5.3.9.3. O pagamento integral do bem no momento da entrega e aceitação dos equipamentos juntamente com a garantia e suporte que irá vigorar por 60 meses a contar da emissão do Termo de Recebimento Definitivo - TRD.

5.3.9.4. O entendimento do TCU é de que a garantia é entregue no momento da ativação; sendo assim, é possível o pagamento à vista embutida no bem e concomitante início da contagem da prestação do serviço de garantia. Ademais, assevera-se que a Orientação Normativa Nº 51 da AGU esclarece que a garantia ultrapassa, geralmente, a vigência do contrato: *in verbis*:

ORIENTAÇÃO NORMATIVA Nº 51, DE 25 DE ABRIL DE 2014 (*)

"A GARANTIA LEGAL OU CONTRATUAL DO OBJETO TEM PRAZO DE VIGÊNCIA PRÓPRIO E DESVINCULADO DAQUELE FIXADO NO CONTRATO, PERMITINDO EVENTUAL APLICAÇÃO DE PENALIDADES EM CASO DE DESCUMPRIMENTO DE ALGUMA DE SUAS CONDIÇÕES, MESMO DEPOIS DE EXPIRADA A VIGÊNCIA CONTRATUAL."

REFERÊNCIA: Arts. 57, 69 e 73, §2º, da Lei nº 8.666, de 1993; PARECER PGFN/CJU/COJLC/Nº 1759/2010.

LUÍS INÁCIO LUCENA ADAMS" (GRIFO NOSSO)

5.3.9.5. Não obstante, a equipe de planejamento da contratação sugere que o contrato seja pactuado pelo período de 12 meses e todos os produtos devem ter garantia embutida pelo período de 60 meses para fins de prestação de serviço relacionado à garantia e suporte.

6. REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

6.1. PARA A SOLUÇÃO DE ESPAÇO DE TRABALHO VIRTUAL

6.1.1. A Solução ID 2, "Solução de VPN para acesso remoto", é considerada inviável pelos seguintes motivos: o uso de conexão VPN (Virtual Private Access), foi explorado neste ETPC e seus riscos às aplicações e dados do INCRA, visto que para esse tipo de solução, o usuário pode acessar de qualquer lugar via conexão remota, e ainda deve-se preocupar com a saúde do dispositivo utilizado, o que seria inviável financeiramente – já que necessitaria de soluções específicas – e tecnologicamente manter o controle. Caso alguma máquina utilizada para acesso remoto seja comprometida, facilmente algum agente malicioso poderia ter acesso à rede de dados do INCRA, colocando em extremo risco tudo ali presente. **Logo, foi descartado por esse motivo e todos os outros apresentados neste ETPC.**

6.2. PARA A SOLUÇÃO DE AGREGAÇÃO E BALANCEAMENTO DE LINKS

6.2.1. A Solução ID 2, "Aquisição de Link MPLS extra sem alta disponibilidade para as localidades remotas", trata-se da simples aquisição de um link extra para conectividade. Essa modalidade não há como ser considerada, uma vez que a inclusão de um link extra não irá resolver problemas de disponibilidade de conexão. Para que a conexão seja balanceada e esteja sempre disponível, além de um segundo link de conexão, faz-se necessário o uso de alguma tecnologia que realize o balanceamento desta conexão.

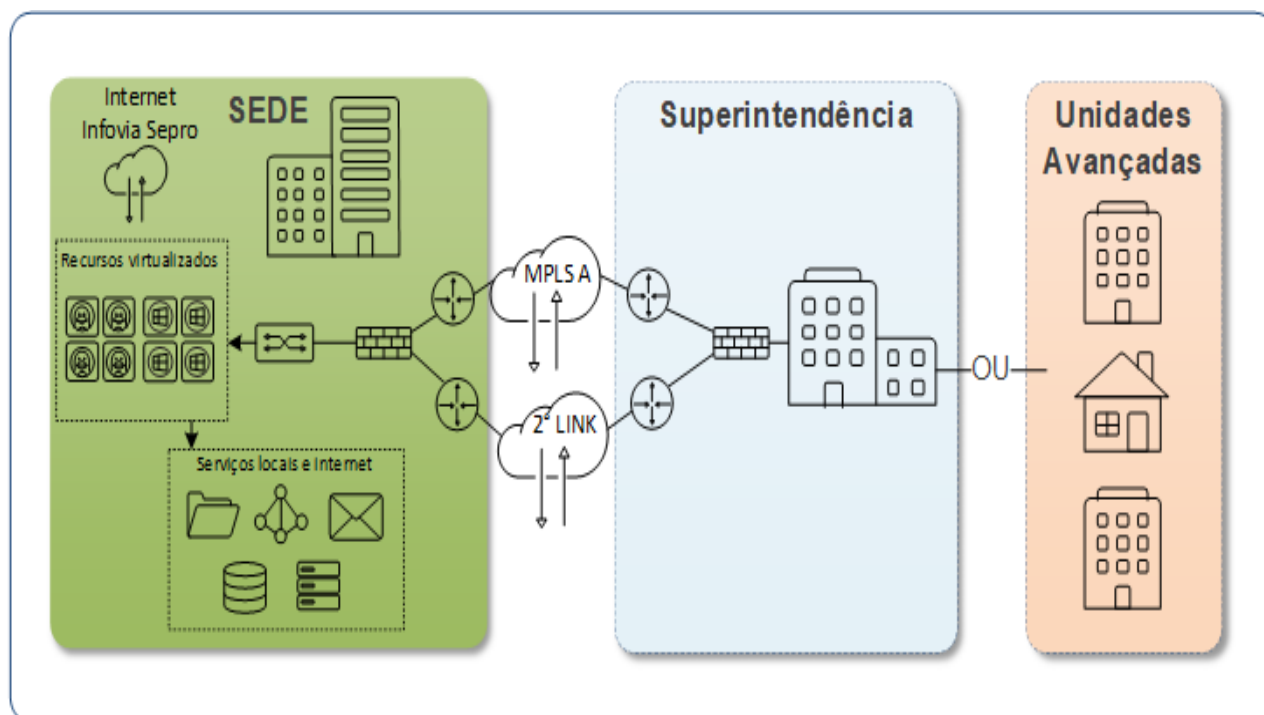


Figura 17: Topologia de conexão com link MPLS extra.

6.2.1.1. Como demonstrado na topologia anterior, em tese, não existe componente capaz de realizar a alta disponibilidade dos links. **Logo, foi descartado por esse motivo e todos os outros apresentados neste ETPC.**

6.2.2. A Solução ID 3, "Aquisição de Link extra sem A Solução ID 2, "Aquisição de Link extra com alta disponibilidade via solução de software livre". Esta solução foi descartada devido às suas características explícitas em contraponto com as necessidades descritas neste ETPC. Tal solução baseada em software livre, uma máquina Linux, seria o componente responsável pela alta disponibilidade das conexões. Na prática, esse componente apenas identificaria uma falha de conexão e transferiria para outro link disponível. Isso aconteceria com alguns segundos de diferença, geralmente causando certa indisponibilidade. Além disso, a solução não possui inteligência suficiente para identificar durante o tráfego dos pacotes de dados uma falha prévia, onde os pacotes começam a se perder, e antes mesmo do link ficar completamente indisponível, a solução já estaria trafegando dados por outro caminho de conexão. Neste cenário ainda seria necessário a manutenção de datacenters espalhados por todas as unidades remotas para que mantivessem a estrutura de software livre para realizar as atividades de "balanceamento". Por fim, apenas de aparentemente resolver os problemas de balanceamento da conexão, esse cenário não seria capaz de conectar as unidades de uma forma ágil e de gestão simples, sendo necessário utilizar ainda conexões VPN site-to-site entre as unidades remotas e o INCRA Sede. **Logo, foi descartado por esse motivo e todos os outros apresentados neste ETPC.**

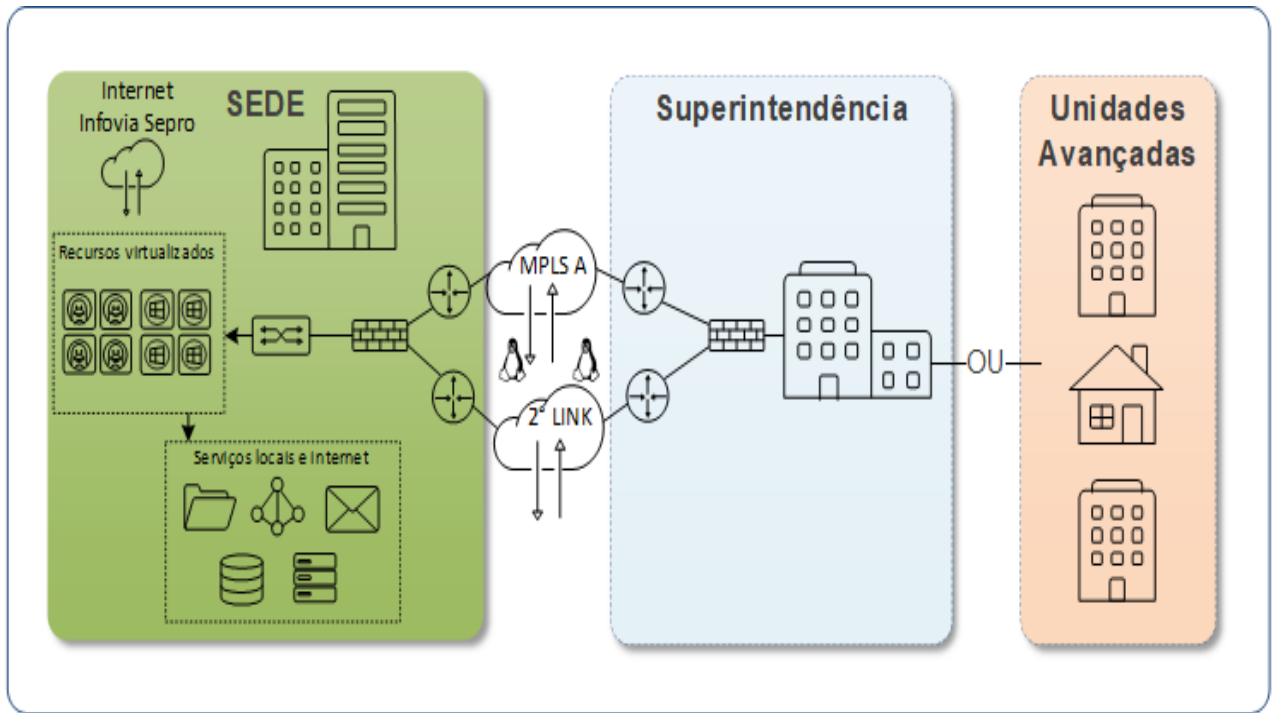


Figura 18: Topologia de conexão com link extra e balanceamento via Linux.

6.3. PARA O FORNECIMENTO DE LINKS DE INTERNET

6.3.1. O fornecimento de links citado na Solução ID 1, é a única solução disponível no mercado para atender às necessidades do INCRA.

7. DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA

7.1. SOLUÇÃO DE ESPAÇO DE TRABALHO VIRTUAL

7.1.1. Solução ID 1, Espaço de Trabalho Virtual Seguro, conforme descrito anteriormente e conforme Anexo I – ETPC (10012570).

7.2. SOLUÇÃO DE AGREGAÇÃO E BALANCEAMENTO DE LINKS

7.2.1. Solução ID 1, Agregação e balanceamento de links, em dois modelos específicos (para SEDE e UNIDADES REMOTAS), conforme descrito anteriormente e conforme Anexo I – ETPC (10012570).

7.3. SERVIÇO DE LINK DE INTERNET REDUNDANTE

7.3.1. Solução ID 1, Link de Internet Redundante, conforme descrito anteriormente e conforme Anexo I – ETPC (10012570).

7.4. TABELA DE ITENS E GRUPOS

GRUPO 1			
ITEM	DESCRIÇÃO	UND	QTD
1	Solução de Espaço de Trabalho Virtual	Usuário	6000
2	Implantação e Repasse de Conhecimento	Serviço	01
GRUPO 2			
ITEM	DESCRIÇÃO	UND	QTD
1	Agregação e Balanceamento de Links Tipo 1 (SR's, UA's e UAE's)	Appliance	77
2	Agregação e Balanceamento de Links Tipo 2 (SEDE)	Appliance	02
3	Implantação e Repasse de Conhecimento	Serviço	01
GRUPO 3			
ITEM	DESCRIÇÃO	UND	QTD
1	Link de Internet 01 - 20Mbps	Link	77
2	Link de Internet 02 - 20Mbps Redundante	Link	77

Tabela disposição de itens para aquisição.

8. ESTIMATIVA DO CUSTO DA CONTRATAÇÃO (IN SGD/ME Nº 01/2019, ART.11, INCISO III)

8.1. Pesquisa de preço ocorrerá após cotação da solução.

9. CUSTO TOTAL DE PROPRIEDADE (IN SGD/ME Nº 01/2019, ART.11, INCISO IV)

9.1. O custo total de propriedade depende da estimativa de custo da contratação.

9.2. A análise comparativa dos custos totais de propriedade (TCO – Total Cost of Ownership) é realizada por meio da comparação do total de gastos acumulados durante determinado intervalo temporal para cada solução, reduzindo-os a valor presente.

10. DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO (IN SGD/ME Nº 01/2019, ART.11, INCISO IV)

10.1. Declara-se por meio deste documento (onde estão demonstrados os benefícios a serem alcançados em termos de eficácia, eficiência, efetividade e economicidade), a viabilidade da contratação por meio da solução escolhida.

11. APROVAÇÃO E ASSINATURA

11.1. A Equipe de Planejamento da Contratação foi instituída pela Portaria 1042/2021 (9477287).

11.2. Conforme o § 2º do Art. 11 da IN SGD/ME nº 01, de 2019, o Estudo Técnico Preliminar (este documento) está aprovado e assinado pelos Integrantes Técnicos e Requisitantes e pela autoridade máxima da área de TIC:

(Assinado Eletronicamente)

Pedro Paulo Mendes Pereira

Chefe da Divisão de Infraestrutura - DOT-2

Integrante Requisitante

(Assinado Eletronicamente)

Luiz Carlos Araújo da Silva

Coordenador Geral de Tecnologia e Gestão da Informação - DOT

Integrante Requisitante Substituto

(Assinado Eletronicamente)

Thomaz Saulo da Silva natividade

Assistente Técnico

Integrante Técnico

(Assinado Eletronicamente)

Laércio Lúcio Pereira Lima

Artífice de Artes Gráficas

Integrante Técnico Substituto

11.3. Ciente e de acordo com os fatos e motivos expostos. Atesto a viabilidade desta contratação e aprovo, na condição de Autoridade máxima da Área de TI, este ETPC conjuntamente com seus anexos que foram elaborados pela EqPC designada pela Portaria 1042/2021 (9477287).

(Assinado Eletronicamente)

Adriano Varela Galvão

Diretor de Gestão Operacional - DO

Autoridade da Área de TI



Documento assinado eletronicamente por **Pedro Paulo Mendes Pereira, Integrante Requisitante - EPC**, em 18/10/2021, às 20:47, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **Thomaz Saulo da Silva Natividade, Integrante Técnico - EPC**, em 18/10/2021, às 20:47, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **Luiz Carlos Araújo da Silva, Coordenador(a)-Geral**, em 18/10/2021, às 21:15, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



A autenticidade deste documento pode ser conferida no site https://sei.incra.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **9946302** e o código CRC **641E9E5B**.