Relatório de acompanhamento e avaliação da evolução de *OpenRAN*

Recursos à Prestação

ANATEL

Acompanhamento e avaliação – *OpenRAN*

Subsídios para o desenho da próxima Agenda Regulatória

Agência Nacional de Telecomunicações
SAUS Quadra 06 Blocos C, E, F e H
CEP 70070-940 Brasília/DF
Telefone (61) 2312-2000

Presidente

Carlos Manuel Baigorri

Conselho Diretor

Alexandre Reis Siqueira Freire
Artur Coimbra de Oliveira
Moisés Queiroz Moreira
Vicente Bandeira de Aquino Neto

Superintendente de Outorga e Recursos à Prestação – SOR

Vinicius de Oliveira Caram Guimarães

Gabinete do Conselheiro Alexandre Freire

Luiza Maria Thomazoni Loyola Giacomin

Superintendência de Outorga e Recursos à Prestação – SOR

Daniel Hindemburg de Miranda Marques
Davison Gonzaga da Silva
Kim Moraes Mota
Maria Aparecida Muniz Fidelis da Silva
Nélia Batista Ferreira Caetano
Rafael Andre Baldo de Lima
Takeshi Ikeda
Thiago Barçante Teixeira

Superintendência de Fiscalização – SFI

Carlos Alberto Dalmolin
Deives Dener de Oliveira
Eduardo Hiroshi Murakami
José Umberto Sverzut
Marcelo Tapajoz Arruda
Ricarda Carolina Rende
Robson Costa Bentes

Superintendência de Controle de Obrigações - SCO

Daniel Adamenas de Andrade
Vanessa Copetti Cravo

Superintendência de Planejamento e Regulamentação – SPR

Rafael Andrade Reis de Araujo

Superintendência de Relações com Consumidores – SRC

Humberto Bruno Pontes Silva

Assessoria Internacional - AIN

Alexandre Campos Moraes

Assessoria Técnica - ATC

Paulo Rodrigo de Moura

Este relatório é desenvolvido pela Superintendência de Outorga e Recursos à Prestação. Possíveis opiniões expressas neste trabalho são exclusivamente do(s) autor(es) e não refletem necessariamente a visão da Agência Nacional de Telecomunicações.

SUMÁRIO

1. Assunto 4
1.1. Definições 4
1.2. Conceito da arquitetura *OpenRAN* 5
2. Grupo de Trabalho de avaliação e acompanhamento da arquitetura *OpenRAN* 6
2.1. Plano de Trabalho 7
2.1.1. Subgrupo 1 – Metas do Eixo Tecnológico 7
2.1.1.1. Subgrupo 1A – Interoperabilidade 7
2.1.1.2. Subgrupo 1B – Segurança 7
2.1.2. Subgrupo 2 – Metas do Eixo Econômico 8
2.1.3. Subgrupo 3 – Metas do Eixo Regulatório 8
2.2. Metodologia 9
2.2.1. Etapa 1 - Mapeamento 9
2.2.2. Etapa 2 - Análise 10
2.2.3. Etapa 3 - Proposição 10
2.2.4. Etapa 4 - Discussão 10
3. Benchmark 11
3.1. Reino Unido 11
3.2. Estados Unidos da América 12
3.3. Índia 14
3.4. Japão 14
3.5. Alemanha 15
3.6. Peru 15
3.7. Colômbia 15
3.8. Indonésia 16
4. Arquitetura *OpenRAN* 17
4.1. Cenário para a problematização da abordagem *OpenRAN* e seus principais *players* 17
4.1.1. Rede Aberta 17
4.1.2. Rede Inteligente 18
4.1.3. Rede Virtual 18
4.1.4. Interoperabilidade de Rede 19

4.1.5. Panorama Atual 19
4.1.6. Padronização 19
4.2. Arquitetura e Interfaces 20
4.3. Topologias e *splits* 24
4.3.1. *Splits* mais recomendadas 27
4.3.2. Topologias 29
4.3.3. *OpenRAN* e soluções customizadas 33
5. Etapa 1 – Mapeamento 34
5.1. TED 35
5.2. GT *OpenRAN* 35
5.3. Das reuniões do GT Técnico e projetos que serão acompanhados 35
5.4. Questões levantadas por *players* nas reuniões bilaterais 35
5.5. Segurança 38
5.6. Ações a serem propostas e em andamento pelo Governo Federal 38
6. Etapa 2 – Análise 38
6.1. Subgrupo 1A – Interoperabilidade 38
6.1.1. Teste de integração e interoperabilidade 39
6.1.2. Histórico de interoperabilidade no âmbito da Anatel 40
6.1.3. Especificações 40
6.1.4. Plataforma RIC 42
6.1.5. Interoperabilidade – Conclusão e aspecto futuro 44
6.2. Subgrupo 1B – Segurança 45
6.2.1. Segurança de Redes 47
6.2.2. *Zero Trust Architecture* 49
6.2.3. ZTA em redes de acesso 51
6.2.4. ZTA em *OpenRAN* 52
6.2.5. ZTA em *Kubernetes* 54
6.2.6. Avaliação de segurança em processos produtivos 56
6.2.7. Segurança – Conclusão 56
6.3. Subgrupo 2 – Aspectos Econômicos – Potenciais Ganhos Econômicos com *OpenRAN* 57
6.3.1. Custos da Rede 58
6.3.2. Estudos de casos mundiais 67
6.3.3. Análise do mercado de fornecedores tradicionais de equipamentos RAN 70
6.4. Subgrupo 3 – Aspectos Regulatórios 72

6.4.1. Macro-eixo Tecnológico - Interoperabilidade 74
6.4.2. Macro-eixo Tecnológico - Segurança 76
6.4.3. Macro-eixo Econômico 78
7. Etapa 3 – Proposição 79
7.1. *Sandbox* regulatório 79
7.2. Localização de *data centers* 83
7.3. Perfis de interoperabilidade 84
7.4. Requisitos de cibersegurança 87
8. Conclusões 95
8.1. Iniciativas Correlatas 95
8.2. Comentários Finais 97

Índice de ilustrações

Figura 1 – Arquitetura *OpenRAN* (https://tinyurl.com/yjy4ao4e) 20
Figura 2 – Interfaces da arquitetura *OpenRAN* (https://tinyurl.com/yjy4ao4e) 22
Figura 3 – Segregação da BBU (https://tinyurl.com/yhx9xf8y) 25
Figura 4 – Opções de *splits* (https://tinyurl.com/yhx9xf8y) 25
Figura 5 – Taxa de bits no *fronthaul* vs. *splits* (https://ieeexplore.ieee.org/document/8479363) 26
Figura 6 – *Tradeoff* para diferentes *splits* (https://tinyurl.com/yhluuug2) 27
Figura 7 – Topologias possíveis 30
Figura 8 – TCO vs. custos de transporte 31
Figura 9 – Capex, Opex e TCO vs. custos de transporte para HTC 32
Figura 10 – Capex, Opex e TCO vs. custos de transporte para LTC 32
Figura 11 – *Near-edge deployment* (https://tinyurl.com/yfhcjad6) 37
Figura 12 - Instalação centralizada do *near* RT RIC 44
Figura 13 - Instalação distribuída do *near* RT RIC 44
Figura 14 – diagrama em blocos de arquitetura *Zero Trust* 55
Figura 15 - Exemplo de Capex de empresa de telecomunicações 58
Figura 16 - Exemplo de Opex de empresa de telecomunicações 58
Figura 17 - Detalhamento do Capex de RAN 59
Figura 18 - Detalhamento do Opex de RAN 60
Figura 19 - Ganhos de Capex com a virtualização da RAN 61
Figura 20 - Ganhos de Opex com a virtualização da RAN 61
Figura 21 - Ganhos de Opex no *backhaul* 62
Figura 22 - Custos de RAN vs. *OpenRAN* em ambiente urbano 63
Figura 23 - ARPU SMP pré e pós no Brasil 64
Figura 24 - Receita *OpenRAN* 65
Figura 25 - Benefícios *OpenRAN* e impactos econômicos 66
Figura 26 - Configuração de receitas *OpenRAN* 67
Figura 27 - Casos de uso mundiais de redes abertas 68
Figura 28 - *Market share* de redes de acesso 71
Figura 29 - *Market share* de redes de acesso no Brasil 71
Figura 30 - Interfaces *OpenRAN* 86
Figura 31 - Conceito de certificação e *badging* da O-RAN *Alliance* 87
Figura 32 - Guia de seleção do esquema de certificação NESAS CCS-GI 94

1. ASSUNTO

Relatório sobre o acompanhamento e avaliação da evolução da *OpenRAN* – (*Open Radio Access Network*, Rede Aberta de Acesso via Rádio) a fim de subsidiar o desenho da próxima Agenda Regulatória, com objetivo de expor a necessidade de ações, em âmbito regulatório, que possam habilitar os potenciais efeitos positivos da arquitetura *OpenRAN*.

1.1. Definições

OpenRAN: Arquitetura de Rede de Acesso via Rádio com padrões de interconexão de módulos predefinidos e *softwares* de fonte aberta. Tem como objetivo permitir redes abertas, inteligentes, virtuais e interoperáveis.

Grupo de Trabalho (GT): Força-tarefa responsável por levantar informações, realizar estudos, discutir os temas relevantes ao assunto *OpenRAN*, acompanhar debates e ações de *players* do mercado com o fim de elaborar relatório demandado pelo Conselho Diretor da Anatel. Formado por membros internos, servidores da Anatel, e membros externos, representantes do mercado. Para tanto, é dividido em etapas intermediárias com entregáveis parciais.

Membros Internos: Servidores da Anatel responsáveis pelos estudos e levantamento de dados que embasarão a elaboração do Relatório Final a ser entregue ao Conselho Diretor.

Coordenador do GT: Membro Interno responsável por reunir e organizar o GT, propondo discussões, centralizando os levantamentos realizados pelos Subgrupos e demandando e recebendo os Membros Externos.

Líderes de Subgrupos: Membro Interno responsável por delegar as tarefas de cada Subgrupo a seus Membros, consolidando as demandas recebidas e as informações levantadas ao Coordenador.

Membros Externos: *Players* do mercado, convidados pelo GT a participarem dos trabalhos oferecendo informações, dados e resultados de testes demandados pelos Membros Internos, na pessoa do Coordenador, e apresentando discussões e sugestões no âmbito do GT.

Prestadoras (ou Operadoras): Empresas prestadoras de serviços de telecomunicações, em especial do Serviço Móvel Pessoal – SMP com interesse em operar a arquitetura *OpenRAN*.

Fornecedoras: Empresas provedoras de tecnologia, seja *hardware* ou *software*, para as Redes de Acesso via Rádio - RAN's das Prestadoras.

Reguladoras Internacionais: Entes públicos, análogos à Anatel, responsáveis pela regulação do mercado de telecomunicações em seus respectivos países que estejam realizando estudos sobre a arquitetura *OpenRAN*.

Academia: Universidades, Institutos de Pesquisa e demais escolas que estejam realizando estudos sobre a arquitetura *OpenRAN*.

Subgrupos: Conjunto de membros internos, entre os quais um líder, com a finalidade de levantar informações e dados para cada macro-eixo de pesquisa.

Macro-eixo de pesquisa: Tema específico, outorgado a cada Subgrupo, que possui uma série de metas relacionadas ao tema que deverão ser estudados. São três os macro-eixos, Tecnológico (subdividido em Interoperabilidade e Segurança), Econômico e Regulatório.

Etapas intermediárias: Ações realizadas por cada subgrupo que deverão produzir resultados em forma de relatórios e apresentação oral, com um cronograma previamente definido, com o intuito de paulatinamente permitir a formatação do Relatório Final a ser entregue ao Conselho Diretor. São quatro as etapas intermediárias, Mapeamento, Análise, Proposição e Discussões.

Relatório Final: Exposição escrita a ser entregue ao Conselho Diretor ao final do prazo de funcionamento do GT no qual que se descrevem todos os fatos e dados colhidos durante os trabalhos realizados pelo Grupo e seus Subgrupos.

O-RAN *Alliance*: Comunidade de operadoras de redes móveis, fornecedores e instituições de pesquisa e acadêmicas que operam na indústria de rede de acesso via rádio (RAN) com o intuito de estimular *OpenRAN*.

Telecom Infra Project (TIP): Comunidade de empresas e organizações que trabalham para acelerar o desenvolvimento e a implantação de redes abertas.

Open Network Automation Platform (ONAP): Estrutura de código aberto, orquestração e automação hospedada pela Fundação Linux.

European Telecommunications Standards Institute (ETSI): Instituto europeu cujo objetivo é definir padrões ao mercado europeu de telecomunicações.

Brownfield: áreas onde já existe uma implantação física industrial e comercial.

Greenfield: área que não possui restrições impostas por trabalho anterior.

Small Cell Forum (SCF): Organização de associação global comprometida em oferecer suporte a infraestrutura móvel ágil e de baixo custo por meio de *small cells*.

Open Networking Forum (ONF): Consórcio destinado a promover redes definidas por *software* e padronizar o protocolo *OpenFlow* e tecnologias relacionadas.

Open RAN *Policy Coalition*: Grupo de empresas formado para promover políticas que promoverão a adoção de soluções abertas e interoperáveis.

Handover (HO): Procedimento empregado em redes sem fio para tratar a transição de uma unidade móvel de uma célula para outra de forma transparente ao utilizador.

Throughput: Taxa de entrega de mensagens em um canal de comunicação.

1.2. Conceito da arquitetura *OpenRAN*

OpenRAN é um conceito de RAN (*Radio Access Network* – Rede de Acesso via Rádio) aberta, inteligente, virtual e interoperável. Para alcançar este objetivo, presume-se

hardwares com interconexão padronizada e *softwares* de fonte aberta. Assim, módulos de diferentes fornecedores podem ser combinados devido à interface aberta e em nuvem.

Conforme Análise nº 13/2021/CB (SEI nº 6500863, Processo SEI nº 53500.004083/2018-79):

> (...) a rede será configurável por software e dividida entre hardware de uso geral e hardware especializado, de uma maneira que permita o posicionamento ideal das funções de rede. Essa flexibilidade, bem como a possibilidade de utilizar hardwares "não proprietários", se coaduna com a intenção de reduzir os custos de hardware e a dependência de um único fornecedor, viabilizando a emergência de iniciativas em torno do chamado Open Radio Access Network (Open-Ran).
>
> Embora ainda incipiente, o Open RAN traz a possibilidade de desenvolvimento de questões de virtualização de funções de rede e redes definidas por software, conceitos que são inerentes ao 5G, a quinta geração das comunicações móveis, além de permitir novas opções de configuração de redes, com redução de custos e menor dependência em relação a um fornecedor específico. De forma mais específica, o Open RAN diminuirá os custos dos equipamentos para o operador de rede porque a rede 5G terá "caixas", cujas funções serão definidas por software. Ao se criar "caixas" mais genéricas, permite-se reduzir partes da eletrônica (hardware) e se possibilita a transferência de inteligência via software, implicando diminuição de custos e a dependência de equipamentos proprietários. Adicionalmente, abre-se a oportunidade de incluir novos players nesse desenvolvimento de equipamentos, ampliando o número de agentes no ecossistema de desenvolvimento e oferta de equipamentos.

O conceito *OpenRAN*, desta forma, se contrapõe ao conceito amplamente difundido no mercado atual de redes de acesso, baseado em soluções proprietárias.

2. GRUPO DE TRABALHO DE AVALIAÇÃO E ACOMPANHAMENTO DA ARQUITETURA *OPENRAN*

Por meio da Análise nº 13/2021/CB (SEI nº 6500863, Processo SEI nº 53500.004083/2018-79) foi decidido que a Superintendência de Outorgas e Recursos à Prestação (SOR) coordenasse grupo para acompanhar e avaliar as ações que estão ocorrendo em outros países e todo o setor, com os seguintes objetivos:

- Efetuar estudo e acompanhamento do tema *OpenRAN* acompanhando debates internacionais e ações das prestadoras, fabricantes e academia.
- Expor a necessidade de ações, em âmbito regulatório, que possam habilitar os potenciais efeitos positivos do *OpenRAN*.

2.1. Plano de Trabalho

É necessário estudar o tema acompanhando debates internacionais e ações das prestadoras, fabricantes, reguladores internacionais, academia e demais *players* do mercado de telecomunicações. Por ser um assunto de grande abrangência, apresenta-se a divisão em três subgrupos, os quais cada um ficou responsável por aprofundar alguns itens do plano de trabalho.

2.1.1. Subgrupo 1 – Metas do Eixo Tecnológico

2.1.1.1. Subgrupo 1A – Interoperabilidade

a) Estado da Arte do *OpenRAN*

Estudo sobre os mecanismos intrínsecos do conceito e das iniciativas *OpenRAN* que permitam a diversificação de atores (nacionais/nacionalizados) e seus impactos positivos e negativos no fornecimento de soluções de *hardware*, de *software*, de aplicações e de integração de sistemas nos diferentes ambientes do 5G: *indoor*, denso-urbano, urbano, suburbano, rural e industrial.

b) *Profiles* no *OpenRAN*

Estudo sobre os requisitos mínimos de interoperabilidade levando em consideração as definições da O-RAN *Alliance*, 3GPP e ONAP, no qual abrange também a definição de *Profiles* dentro do *OpenRAN* tanto para os cenários de eMBB (*enhanced Mobile Broadband*, Banda Larga Móvel Melhorada) com FR1 (banda de frequências entre 4,1 GHz e 7,125 GHz usada para transportar a maior parte do tráfego tradicional de comunicações móveis celulares) e FR2 (banda de frequências entre 24,25 GHz a 52,6 GHz focada em recursos de alta taxa de dados de curto alcance), URLLC (*Ultra-Reliable Low-Latency Communication*, Comunicação ultra confiável de baixa latência) com FR1 e FR2 e mMTC (*massive Machine-Type Communication*, Comunicação Maciças do Tipo Máquina) com FR1 e FR2.

c) Interoperabilidade para nova tecnologia

Estudo sobre diretrizes e critérios a serem atendidos em testes de novas tecnologias para o cenário 5G/6G, que garantam interoperabilidade entre sistemas-chave, inteligência e transparência (*openness*).

d) Arquitetura *OpenRAN* em redes com tecnologia 4G ou inferiores

Estudo que analisa as arquiteturas utilizadas em outros países para operacionalização tecnológica do 5G com abordagem *OpenRAN*. Os impactos tecnológicos da manutenção de redes legadas (2G, 3G, 4G e, até mesmo, 5G) na implementação efetiva de soluções inovadoras fundadas no conceito *OpenRAN*.

2.1.1.2. Subgrupo 1B – Segurança

e) Requisitos de segurança das soluções de *OpenRAN*

Neste ponto se elabora estudo com debates acerca dos aspectos de segurança que deverão ser incorporados à arquitetura, esse tópico recentemente foi debatido nos fóruns internacionais (ex. SONIC, *SmartRAN Open Network Interoperability Center*, um ambiente comercialmente neutro e colaborativo para testar a interoperabilidade e a integração de soluções de rede abertas, desagregadas e centradas em software e arquiteturas de vários fornecedores no Reino Unido), bem como eventuais riscos à segurança e integridade da segurança nas comunicações.

2.1.2. Subgrupo 2 – Metas do Eixo Econômico

a) Impactos do *OpenRAN* no mercado de telecomunicações

Estudo sobre os possíveis impactos que a iniciativa *OpenRAN* pode influenciar nos custos dos equipamentos das prestadoras de serviços de telecomunicações, inclusive abordando eventual aumento ou redução de custos das prestadoras na implantação da rede, diminuição na dependência de fornecedores específicos e se poderá resultar em menores ou maiores preços para os consumidores.

b) Valores Agregados pela *OpenRAN* na indústria

Estudo econômico sobre como a indústria brasileira de telecomunicações pode "agregar valor" ao mercado brasileiro, melhorando sua competitividade por meio da iniciativa *OpenRAN*, bem como o modelo de código aberto ou de interface aberta, abordando as diretrizes e critérios na definição de métricas que identifiquem, considerando dados reais, níveis de eficácia, de confiabilidade, de competitividade entre fornecedores, de impacto financeiro, de desempenho e de diversidade de fornecedores provocados pelo *OpenRAN* e outros conceitos afins.

c) Necessidade de capacitação de mão de obra

Estudo sobre a necessidade de qualificação de mão-de-obra no Brasil para produzir e implementar elementos de rede propostas na iniciativa *OpenRAN* e avaliar como a iniciativa poderá fomentar capacitação de recursos humanos no Brasil.

2.1.3. Subgrupo 3 – Metas do Eixo Regulatório

a) Estudo sobre eventuais barreiras legais e infra legais ao desenvolvimento do *OpenRAN*

Nesta etapa, se desenvolve estudo sobre eventuais barreiras legais e infra legais que impactem na implementação efetiva de soluções inovadoras fundadas no conceito *OpenRAN*, inclusive questões afetas a direitos autorais e registro de patentes.

b) Propostas de Política Pública

Entrega de estudos sobre possíveis instrumentos para incentivos públicos e regulatórios, para aparecimento e o amadurecimento de novas tecnologias disruptivas, que incluam, entre outras, a alavancagem de PD&I.

2.2. Metodologia

Os trabalhos dos Membros Internos são realizados no âmbito dos Subgrupos predefinidos. O Coordenador define com os Líderes de Subgrupos as tarefas a serem realizadas seguindo as etapas descritas em sequência. Os Subgrupos, por meio de seus Líderes, demandam o Coordenador para que este consolide as questões a serem enviadas aos Membros Externos, assim como este receberá as respostas e repassará aos Subgrupos por meio de seus Líderes. Tais trocas de informações embasam a elaboração dos resultados parciais.

Neste trabalho, adotou-se uma série de etapas consecutivas para possibilitar a implementação do estudo exploratório, objeto deste projeto. São elas: mapeamento, análise, proposição e discussão. Ao final de cada etapa foram produzidos, como entregáveis do projeto, os resultados obtidos, na forma de relatório e apresentação oral.

2.2.1. Etapa 1 - Mapeamento

Na etapa de mapeamento, o foco recai na imersão sobre as temáticas nucleares do projeto, com vistas ao delineamento conceitual, à consciência situacional e à compreensão dos elementos constituintes do problema de pesquisa. Inicia-se abrangendo a definição do problema em si, a fundamentação teórico-conceitual, as expectativas das partes interessadas, as outras soluções tecnológicas já disponíveis e as implicações do *OpenRAN* para a indústria e o mercado de telecomunicações.

Esse processo de descoberta de conhecimento é realizado por meio da imersão aos eixos temáticos, identificando várias perspectivas presentes e situações particulares que fazem parte dos diferentes contextos e domínios que se encerram na implementação do *OpenRAN*.

Nesta etapa, busca-se aliar os aspectos teóricos e os aspectos técnicos que subjazem a definição do *OpenRAN*, com os princípios e a visão dos diferentes arranjos da arquitetura técnica.

Ao longo do mapeamento, as equipes de pesquisadores se aproximam do domínio do problema e esclarecem os eixos temáticos, além de dimensionar o alcance das linhas de base das pesquisas. Inicia-se com pesquisas e levantamento de artefatos de informação básicos sobre os eixos temáticos.

Por fim, as equipes de pesquisa ampliam os horizontes de estudo para poder explorar os contextos histórico, tecnológico, regulatório e mercadológico. Visa, portanto, encontrar todos os pontos de partida que podem gerar *insights* para a continuidade do projeto de pesquisa básica em curso.

Ao final desta etapa, como entregável, apresenta-se um relatório e realiza-se uma apresentação oral, contemplando uma visão holística, que possibilite a compreensão multidisciplinar das diferentes perspectivas de interesse das partes envolvidas e afetadas, considerando cada eixo temático.

2.2.2. Etapa 2 - Análise

De posse dos artefatos coletados na etapa de mapeamento, as equipes de pesquisadores estão aptas a proceder a análises sob diferentes perspectivas, de modo a evidenciar os diferentes pontos de vista e os diferentes contextos de pesquisa. Foi conduzida usando uma ampla gama de métodos, estruturas teóricas e análises conceituais. A título ilustrativo, as seguintes abordagens foram empreendidas para proceder às análises qualitativas sobre os eixos temáticos, incluindo: análise documental, análise de conteúdo, análise do discurso, revisão sistemática e desenvolvimento e análise de opções estratégicas.

A análise qualitativa visava a obter alguma forma de explicação, compreensão ou interpretação dos fenômenos e fatos que deram origem e que são decorrentes da arquitetura *OpenRAN*.

Ao final desta etapa, como entregável, gera-se um relatório e realiza-se uma apresentação oral, em que as equipes de pesquisadores buscarão responder a perguntas sobre "o quê", "por quê", "como", "de que forma", "em que circunstâncias" etc., com relação à problemática de cada tema proposto.

2.2.3. Etapa 3 - Proposição

Após obter um grande volume de informações e *insights*, advindos das etapas anteriores, chega-se o momento de consolidar as análises a fim de se produzir uma síntese dos diferentes eixos temáticos. Avaliar o caminho a seguir e identificar cenários de uso e de implementação das tecnologias e frameworks *OpenRAN* são importantes instrumentos para identificar potenciais desafios e adequações tecnológicas, regulatórias e configurações de valor no âmbito da indústria e do mercado de Telecomunicações.

A partir da reflexão e compreensão das possibilidades e dos modelos de implementação que emergem do arcabouço tecnológico do *OpenRAN* no cenário brasileiro, hipóteses foram formuladas e novas realidades puderam ser projetadas a partir da transformação tecnológica desencadeada.

Neste momento, abre-se espaço para o "caos criativo", que culmina, ao final desta etapa, com os entregáveis (relatório e apresentação oral), contemplando o delineamento das principais descobertas e achados em cada eixo temático. Pode-se identificar os potenciais fatores habilitadores para impulsionar *OpenRAN* no Brasil, primando pelos domínios estratégicos e operacionais e pelas potencialidades e condicionamentos – oportunidades e desafios que lhe são inerentes, em cada linha temática proposta.

2.2.4. Etapa 4 - Discussão

Na etapa de discussão concentram-se as informações relevantes obtidas a partir do mapeamento conceitual e da fundamentação teórica-técnica, aliadas às análises e proposições subsequentes. Avaliou-se o percurso metodológico e confrontou-se os achados e descobertas dos eixos temáticos ante às principais conjecturas, constatações

e evidências dos fragmentos teóricos e das experienciações do *OpenRAN* em cenários de simulação e de implementação.

Ao final desta etapa, como entregável, gera-se um relatório e realiza-se uma apresentação oral, contemplando as estratégias promissoras de implementação do *OpenRAN*, as pilhas de desenvolvimento tecnológico e os diferentes cenários de prática, alinhados aos resultados obtidos em cada etapa anterior e para cada tema proposto.

Ao final das quatro etapas, apresenta-se ao Conselho Diretor relatório descrevendo os estudos realizados pelo GT com conclusões a fim de embasar as decisões do Egrégio Colégio.

3. *BENCHMARK*

3.1. Reino Unido

O regulador britânico de telecomunicações, *Ofcom* (*The Office of Communications*, O Gabinete de Comunicações), identificou que, com o passar dos anos, o número de fornecedores de equipamentos de rede de acesso para comunicações móveis diminuiu, decrescendo também a concorrência no setor. A fim de superar essas limitações, o governo do Reino Unido implementou uma estratégia de 'diversificação de fornecedores de telecomunicações'. Em termos simples, isso significa [ampliar] a capacidade dos operadores de rede de obter tecnologia de uma gama mais ampla de fornecedores[1].

Nesse sentido, o *Ofcom* tem buscado ações para incentivar a inovação e o investimento em redes, para que as pessoas e as empresas possam contar com serviços rápidos, confiáveis e seguros.

Uma das ações é o projeto SONIC Labs (*SmartRAN Open Network Interoperability Center*), um programa conjunto entre o *Ofcom* e a *Digital Catapult* que ajudará a testar novas soluções potenciais para uso futuro na cadeia de suprimentos de telecomunicações, visa principalmente testar a interoperabilidade e integração de soluções de rede aberta, começando com *OpenRAN*. O SONIC criará uma plataforma para fornecedores existentes e emergentes se reunirem para testar e demonstrar soluções interoperáveis. Especificamente, o Centro buscará: (i) Fornecer às empresas inovadoras um ambiente neutro para se reunirem para testar e demonstrar soluções; (ii) facilitar o teste de interoperabilidade com organizações envolvidas no desenvolvimento de padrões e similares - por exemplo, ETSI, ORAN *Alliance*, *Telecom Infra Project* (TIP); (iii) Apoiar e conectar pequenas e grandes empresas para colaborar em um cenário de rápida mudança tecnológica; (iv) operar em um estágio pré-comercial nos níveis de preparação de tecnologia 5G.

A rede SONIC foi construída em diferentes locais no Reino Unido, para testar opções de tecnologia e aprender quais benefícios ela pode trazer, com funcionamento a partir de maio de 2021.

[1] https://www.ofcom.org.uk/about-ofcom/latest/features-and-news/what-is-open-ran

Outra ação anunciada em julho de 2021[2] se refere à iniciativa financiada conjuntamente pelo Departamento de Digital, Cultura, Mídia e Esporte (DCMS) e *Ofcom*, denominado *Future* RAN *Competition*. Segundo informações nos *sites* do governo inglês trata-se de uma concorrência aberta administrada pela DCMS, que alocará até trinta milhões de libras referente a recursos de fundos de P&D para projetos que estejam relacionados a Estratégia de Diversificação da Cadeia de Suprimentos 5G do governo. Com a referida ação se busca incentivar a indústria britânica a criar produtos e serviços possibilitando haver os potenciais benefícios do *OpenRAN*, inclusive maior inserção na cadeia de fornecimento global emergente com base em padrões abertos.

A Estratégia de Diversificação[3] exige o estabelecimento de um amplo ecossistema de P&D no Reino Unido, abrangendo uma variedade de áreas, incluindo:

- O desenvolvimento de *hardware*;
- *Software* / soluções virtualizadas;
- Teste com redes ao vivo; e
- Aceleração e impulso ao desenvolvimento de tecnologias interoperáveis.

Já existe um ecossistema se formando por meio de financiamento do setor privado. No entanto, o governo britânico entende que esta ação proporcionada pelo setor público ajudará a aproveitar esse impulso, promover a colaboração e reunir os pontos fortes dos setores de P&D do Reino Unido para direcionar aos objetivos da cadeia de abastecimento diversificada que o Reino Unido entende necessários para garantir sua segurança nacional e resiliência. Em última análise, os projetos a serem financiados pelos fundos devem ajudar a desenvolver produtos que resolvam os principais desafios colocados por novas tecnologias interoperáveis e desenvolver a capacidade inicial do Reino Unido no ecossistema *OpenRAN*.

3.2. Estados Unidos da América

A FCC (*Federal Communications Commission*, Comissão Federal de Comunicações) lançou em fevereiro de 2021 um *Notice of Inquiry*[4] solicitando ao público em geral informações a respeito de diversos temas afetos a *OpenRAN*.

Como contribuições recebidas, e que devem estar em análise, são, dentre outras:

- Criação de um programa de certificação da indústria para RAN aberta pode ser um marco significativo, onde todos os fornecedores de componentes são certificados (Microsoft, Ericsson e outros), se possível no modelo de certificação OnGo;

- Instituição, por meio do DoD (*Department of Defense*, Departamento de Defesa) de um laboratório para o qual todos os fornecedores possam levar seus produtos para testes funcionais e de interoperabilidade;

- Criação de um Centro de Teste e Integração Aberto (OTIC), que visaria "testar e verificar a conformidade do equipamento RAN com as

[2] https://www.gov.uk/guidance/future-ran-diversifying-the-5g-supply-chain
[3] https://uk5g.org/5g-updates/research/5g-supply-chain-diversification-strategy/
[4] https://www.fcc.gov/document/fcc-seeks-comment-open-radio-access-networks-0

especificações da interface O-RAN, com base nas especificações de teste de conformidade O-RAN."

A FCC, em coordenação com a NTIA (*National Telecommunications and Information Administration*, Administração Nacional de Telecomunicações e Informações do Departamento de Comércio), anunciou em janeiro de 2021, o programa "Desafio 5G", que afirma ser projetado para "garantir a cooperação, colaboração e interoperabilidade entre os participantes" na busca de " um ecossistema 5G aberto que pode suportar missões DoD. "

Em julho de 2021, a FCC promoveu dois *showcases* com apresentações das ações e equipamentos desenvolvidos por alguns fornecedores com tecnologia aberta. Na oportunidade, a FCC informou que será proposta a criação de zonas de inovação nos Estados Unidos, para que sejam locais de teste de rede sem fio, em parte na tentativa de adicionar mais impulso à tendência de RAN aberta. Os locais de teste em escala municipal designados pela FCC seriam gerenciados pela NSF (*National Science Foundation*, Fundação Nacional de Ciência), a chamada PAWR (*Platforms for Advanced Wireless Research*, Plataformas para Pesquisa Avançada sem Fio). Na proposta consta que Boston abrigará o emulador de rede *Colosseum* da DARPA (*Defense Advanced Research Projects Agency*, Agência de Projetos de Pesquisa Avançados da Defesa), que foi usado no agora concluído *Spectrum Collaboration Challenge* da agência . Raleigh, enquanto isso, vai abrigar a anunciada anteriormente AERPAW (*Aerial Experimentation and Research Platform for Advanced Wireless*, Plataforma de Experimentação e Pesquisa Aérea para Comunicação Avançada sem Fio), que se concentra em comunicações sem fio para drones e outros sistemas aéreos não tripulados.

Este esforço soma-se a duas zonas de inovação existentes, apoiados pela O-RAN *Alliance* - um dos principais grupos de desenvolvimento de padrões para redes RAN abertas – que realizou dois *plugfests* mundiais. O primeiro , no final de 2019, incluiu atividades na zona de inovação da cidade de Nova York, patrocinada pela AT&T. O segundo, realizado perto do final de 2020, incluiu atividades na cidade de Nova York e em Salt Lake City e foi organizada pela AT&T e pela Verizon. Ambos os *plugfests* da O-RAN *Alliance* nos EUA operaram por meio do programa PAWR financiado pela NSF do governo dos EUA.

Há em andamento pela FCC o programa "remover e substituir" da agência para equipamentos Huawei e ZTE, programado para se iniciar em outubro 2021. A agência vem trabalhando nos parâmetros de um programa projetado para alocar quase US$ 2 bilhões em financiamento do Congresso para operadoras de rede dos Estados Unidos que possuem equipamentos Huawei e ZTE em suas redes.

A FCC também tem solicitado estudos sobre o tema, sendo de conhecimento um desenvolvido pela Widelity e outro da Mavenir sobre os custos dos equipamentos de redes abertas.

Outra iniciativa desenvolvida pela administração pública estadunidense é o Fundo Público de Inovação da Cadeia de Suprimentos Sem Fio[5]: US$ 1,5 bilhões por meio da *National Telecommunications and Information Administration* (NTIA), em coordenação com o NIST, o Departamento de Segurança Interna e o Diretor de Inteligência Nacional, entre outros, para estimular o movimento em direção à arquitetura aberta, tecnologias sem fio baseadas em *software*, financiamento inovador, tecnologias de "salto à frente" no mercado de banda larga móvel dos EUA. Em reunião com representantes da NTIA, foi informado que esta linha de financiamento está disponível para entidades de outros países.

3.3. Índia

A Autoridade Indiana, TRAI, entende que as redes de acesso tradicionais estão evoluindo para *OpenRAN* com o aumento da demanda de dados e, por ser baseada em interfaces abertas, *hardware* independente do fornecedor e tecnologia definida por *software*, o desenvolvimento de tecnologia *OpenRAN* facilitaria o compartilhamento ativo da infraestrutura. Para resolver estes cenários emergentes, a Autoridade é de opinião que os provedores de internet devem ser limitados pelas ordens, instruções e regulamentos emitidos pela autoridade competente[6].

Na visão da TRAI, o uso de *OpenRAN* e redes de telecomunicações definidas por *software* abrirá novas oportunidades para as empresas indianas entrarem no mercado de equipamentos de rede[7].

Uma operadora indiana já desenvolveu e testou uma rede de acesso de rádio de quinta geração, atingindo o marco de 1 Gigabit por segundo e planeja acelerar a transição de tecnologia para RAN aberta com arquitetura desagregada[8].

3.4. Japão

No Japão, o governo está oferecendo incentivos fiscais para produtos com interfaces abertas e interoperáveis e o Ministério de Assuntos Internos e Comunicações (MIC – *Ministry of Internal Affairs and Communications*) e delineou planos para buscar colaboração internacional a fim de promover a implementação e padronização de arquitetura aberta e virtualização de rede[9].

[5] https://www.law.cornell.edu/uscode/text/47/906
[6] https://www.trai.gov.in/sites/default/files/Recommendations_13032020.pdf
[7] https://indianexpress.com/article/business/trai-chairman-open-ran-will-present-opportunities-7153590/
[8] https://telecom.economictimes.indiatimes.com/news/openran-to-help-local-telecom-equipment-manufacturing-trai-chairman/80362181
[9] https://www.federalregister.gov/documents/2021/03/29/2021-06430/promoting-the-deployment-of-5g-open-radio-access-networks

3.5. Alemanha

A Alemanha anunciou um pacote de estímulo de € 130 bilhões em junho de 2021 para novas tecnologias digitais, como por exemplo € 5 bilhões para investimentos em inteligência artificial[10].

O fundo de tecnologia de rede designou € 2 bilhões que estão sendo direcionados para desenvolvimentos de *OpenRAN* e espalhados por vários projetos gerenciados por vários órgãos do governo alemão, incluindo o Ministério Federal de Pesquisa, o Ministério dos Transportes, o Departamento Econômico e o Ministério do Interior.

3.6. Peru

O programa peruano Internet para Todos (*IpT Perú*) implantou centros com a tecnologia *OpenRAN* no país para otimizar recursos e baratear operação de telecomunicações. A iniciativa, uma parceria entre Telefónica, Facebook, Banco de Desenvolvimento da América Latina (CAF) e Banco Internacional de Desenvolvimento (BID), tem como objetivo promover a universalização em regiões remotas da nação vizinha, incluindo a porção da Amazônia peruana. A intenção é implantar centenas de zonas 4G *OpenRAN* virtualizadas, mas preparando terreno para o 5G.[11] A distribuição e implantação de baixa densidade nessas regiões trazem alto custo operacional e de investimento, além de adicionar complexidade. A virtualização da rede de acesso ajudaria nesse quesito, mas a intenção é de também ajudar no redimensionamento da capacidade em regiões urbanas.

A rede *OpenRAN* 4G atende 1.762 localidades na região de Huancavelica, Peru. Por meio da infraestrutura do IPT, a região de Huancavelica conta com mais de 158 mil habitantes em áreas rurais e que já possuem acesso à internet 4G. Até o final de 2021, a Telefónica, uma das empresas parceira no projeto, promete que o número chegará a 164 mil habitantes. Salienta-se que Huancavelica é uma das regiões com maiores níveis de pobreza do Peru, de acordo com o Instituto Nacional de Estatística e Informática peruano. No total, as redes do IpT atendem a 30.000 comunidades.

De acordo com as empresas envolvidas, o custo do equipamento eletrônico era a metade nos *sites OpenRAN* do que nos tradicionais. Isso tem sido fundamental para permitir que o IpT atenda a comunidades com baixa renda[12].

3.7. Colômbia

Por meio de sua marca Tigo, o grupo de telecomunicações Millicom está preparando a implementação de uma rede de acesso *OpenRAN* 4G na Colômbia com fornecimento da Parallel Wireless. O projeto utilizará a faixa de 700 MHz em áreas rurais com pouca cobertura. Como integradora de sistemas, a Parallel oferecerá serviços de instalação,

[10] https://www.telecomtv.com/content/open-ran/open-ran-projects-in-line-for-massive-german-government-funds-report-40682/
[11] https://tinyurl.com/yj24yeuc
[12] https://tinyurl.com/ygf795ty

integração e monitoramento de rede. A empresa acredita que o projeto indicará forte desempenho de rede, superando os indicadores-chave de desempenho (Key Performance Indicators, KPIs). A rede *OpenRAN* também estará pronta para futura agregação de serviços 5G. De acordo com a Millicom, a iniciativa pode ser replicada em outros mercados onde a multinacional atua.

3.8. Indonésia

OpenRAN pode ser entendida como a tecnologia capaz de oferecer solução em conectividade a rádio em países em desenvolvimento. Se por um lado, viabiliza a conectividade e serviços nestes países, por outro proporciona o desenvolvimento local da tecnologia de rede. Vale ainda salientar que a *OpenRAN* é liderada pela TIP que busca propagar a comercialização do domínio RAN com produtos e suporte ao desenvolvimento de soluções desagregadoras e interoperáveis. Com o intuito de testar a viabilidade e capacidade do emprego da tecnologia de *OpenRAN*, operadoras móveis na Indonésia colocaram a teste essa tecnologia em seu país.

Não obstante a relativamente grande população e a presença de grandes metrópoles com alta densidade, a Indonésia é um país predominantemente rural dividido em mais de 17 mil ilhas com boa parte de sua população – 61 milhões dos 270 milhões – sem acesso à Internet. Soma-se ao desafio geográfico o desafio do mercado que, em comum com muitos outros mercados em desenvolvimento, os níveis de receita média por cliente são relativamente baixos.

Com o objetivo de ampliar a conectividade local, o TIP criou um TIP *Community Lab* em uma universidade da Indonésia para, através de testes e validação de tecnologias de redes abertas, interoperáveis e desagregadas, implantar soluções viáveis do ponto de vista comercial. Embora a tecnologia *OpenRAN*, com seu viés de desagregação de tradicionais elementos de rede, permita uma diversidade de funções virtuais de rede, tal tecnologia enfrenta uma miríade de obstáculos e dificuldades em sua implementação e testagem na Indonésia.

Não obstante o desafio existente, o TIP *Community Lab* conseguiu executar a tarefa ao optar por uma solução que buscasse se concentrar em testagem e validação de tecnologias em redes abertas e desagregadoras, encontrando, deste modo, soluções comercialmente viáveis.

O projeto do TIP *Community Lab* consistiu em um planejamento de arquitetura de IP, RAN, transporte e núcleo. Para tal, o laboratório foi conectado a dois dos MNOs (*Mobile Network Operator*, Operadora de Rede Móvel) locais usando *backhaul*[13] por micro-ondas e satélite. A infraestrutura do laboratório consistia em equipamentos compatíveis com *OpenRAN* dos fornecedores Parallel Wireless, Mavenir e Aliostar. Já em relação ao transporte, integrou-se à topologia elementos do grupo de projetos TIP OOPT[14], DCSG[15] e Cassini (Transponder).

[13] Interface entre o núcleo e a RAN
[14] *Open Optical Packet and Transport*

A testagem foi orientada pelos padrões O-RAN e 3GPP de modo a garantir que, em todos os casos, as áreas da arquitetura O-RAN fossem testadas e verificadas. A execução dos testes comprovou diversos resultados positivos dentre os quais: chamadas de voz e vídeo usando equipamento *OpenRAN* durante a conexão ao núcleo de rede do MNO´s e Médias de 38 Mbps e máxima de 60 Mbps para downloads e médias de 14Mbps e máxima de 16.4Mbps para uploads com larguras de bandas de 5MHz e 10MHz.

A partir das aplicações e testes no laboratório visando o foco na melhoria, tanto de *greenfield* quanto de *brownfield*, pode-se garantir que a arquitetura simulasse os ambientes do mundo real de modo que as descobertas nos laboratórios reduzissem os riscos e incertezas a respeito de implantações no mundo real, isto é, problemas de interoperabilidade entre fornecedores de *hardware* e *software*. A partir da experiência e dos testes bem-sucedidos do TIP *Community Lab*, algumas operadoras da Indonésia estão acelerando suas atividades *OpenRAN*, com inclusive algumas dessas já participando de testes com a tecnologia *OpenRAN*.

4. ARQUITETURA *OPENRAN*

4.1. Cenário para a problematização da abordagem *OpenRAN* e seus principais *players*

Uma RAN convencional possui todos os módulos, tanto *hardware* quanto *software*, fornecidos por um único fornecedor por meio de uma solução proprietária. É esta característica a primeira a ser atacada pela abordagem *OpenRAN*, haja vista o disposto na Portaria MCOM nº 1.924/2021 (https://tinyurl.com/yhks8v22), que determina o incentivo à interoperabilidade e à arquitetura aberta nas licitações das faixas de radiofrequências de seu escopo.

Detalhando cada uma das quatro características do conceito *OpenRAN* difundidas pelos *players* (https://www.o-ran.org/), pode-se verificar que tal concepção se coaduna com o interesse público já explicitado na Portaria MCOM nº 1.924/2021 e na Análise nº 13/2021/CB.

4.1.1. Rede Aberta

A 5ª geração de comunicações móveis, 5G, prevê uma grande quebra de paradigma em tais comunicações. Se até a 4ª geração o foco era o usuário, começando com tráfego de voz até streaming de vídeo, a 5G tem como foco conectar dispositivos que demandarão comunicação por si sós, como veículos autônomos, sensores, equipamentos residenciais e industriais e tantos outros considerando o advento da Internet das Coisas (IoT, *Internet of Things*), Indústria 4.0, Cidades Inteligentes e Inteligência Artificial.

Desta forma, a desagregação permite que as operadoras de telefonia celular se utilizem de soluções de vários fornecedores para montagem e atualização de suas

[15] *Disaggregated Cell Site Gateway*

redes, e, com tal flexibilidade, as *OpenRAN's* podem se adaptar à diversidade de usos e requisitos 5G.

Espera-se que a arquitetura aberta reduza barreiras à entrada de mais *players* no mercado de comunicações móveis, incentivando a inovação tecnológica do setor, reduzindo passos de desenvolvimento e diminuindo custos, benefícios que podem ser repassados ao usuário final.

Nota-se também que uma rede aberta, por ser mais modular, mais visível e menos interdependente pode incrementar a segurança de rede[16]. Uma rede proprietária deixa o usuário dependente do fornecedor, o único responsável por identificar e combater ameaças à segurança de rede. Contratos expirados podem deixar a operadora de rede sem suporte à segurança. Já a modularização pode fazer com que haja menos descontinuidades na prestação do serviço quando da atualização das redes.

4.1.2. Rede Inteligente

Dispositivos inteligentes conectados a uma rede de comunicação demandam muito dos recursos disponíveis. Por exemplo, a tecnologia RFID (*Radio Frequency Identification*, Identificação por Radiofrequência), utilizada para o controle de movimentação de pessoas em um ambiente e combate a roubos e furtos em lojas, entre outras aplicações, permite que os dispositivos controlados se comuniquem entre si e com uma central sem a ação humana. Expandindo o conceito para Cidades Inteligentes, pode-se imaginar o impacto que o desenvolvimento de tais dispositivos pode causar em redes de comunicações.

A arquitetura aberta permite que as redes dos prestadores de serviços sejam atualizadas de uma maneira mais célere, uma vez que não é necessário haver um dispositivo desenvolvido pelo *vendor lock-in* que possui a tecnologia proprietária da rede, havendo assim um rol de escolhas mais diversificado para os operadores. Atualizações mais frequentes podem proporcionar redes 5G mais avançadas mais rapidamente e com mais soluções para conseguir gerir os serviços oferecidos à sociedade.

Ao adicionar inteligência às redes, é possível fazer adaptações e melhorias sem demandar ação humana, como por exemplo compartilhar infraestrutura com nuvem RAN e outras funções de rede virtualizadas ou otimizar o tráfego por meio de ferramentas de Aprendizado de Máquina.

4.1.3. Rede Virtual

A virtualização da rede permite que muitos dos componentes sejam fornecidos como *software* alocados em um *data center*, substituindo dispositivos físicos. Tais *data centers* podem ser distribuídos ou centralizados, mas independentemente da disposição desses elementos, este conceito introduz uma série de benefícios através da escalabilidade da operadora, que pode aumentar a capacidade da sua

[16] https://tinyurl.com/yhurhkef

rede sem trocar fisicamente os equipamentos quando alcançam a obsolescência. Soluções virtualizadas permitem adaptar a capacidade do *software* e dos processadores nos *data centers*, o que pode ser vantajoso ao se comparar com atualizações realizadas em redes baseadas em dispositivos físicos, que demandam troca de equipamento e substituição de *firmware*, por exemplo.

4.1.4. Interoperabilidade de Rede

A interoperabilidade é o conceito que permite a maior dinâmica no funcionamento de uma *OpenRAN*. Trocar caixas (*white boxes*) desatualizadas por outras mais adaptadas às necessidades da operadora, independentemente de seu fabricante e sua arquitetura interna, com foco apenas na funcionalidade, desde que com interfaces padronizadas, estimula a competição entre fornecedores e incentiva a modernização de redes.

A maior oferta de fornecedores incentiva os aspectos de interoperabilidade entre portadoras da *OpenRAN*, além de poder aumentar a eficiência de redes 4G existentes, pois elas continuam a incorporar a virtualização e a desagregação, características valorizadas em redes 5G.

Salienta-se que as instituições que trabalham na padronização da arquitetura *OpenRAN*, como O-RAN *Alliance* e *Telecom Infra Project* (TIP) têm disponibilizado plataformas para testes de verificação de conexão a seus associados[17].

4.1.5. Panorama Atual

Com a implementação da 5G no Brasil, espera-se redes com maior velocidade, maior tráfego e menor latência. Este incremento de capacidade demanda maior quantidade de recursos, em especial espectro de radiofrequências. Isso causou alguns conflitos, em especial sobre a convivência da 5G com o serviço de TVRO (*television receive only*, canais abertos de TV por satélite), que usa a banda C.

Além da competição por recursos, há também discussões sobre a padronização das redes. Além do modelo *OpenRAN*, no mercado há também a opção do modelo *SingleRAN*, com soluções proprietárias como são atualmente as redes existentes. Inclusive alega-se a possibilidade de a arquitetura *OpenRAN* atrasar a implementação das redes 5G no Brasil, devido a sua baixa maturação.

4.1.6. Padronização

Mais do que promover uma plataforma aberta, a arquitetura *OpenRAN* determina padrões de interfaces entre diferentes módulos. É essa característica que permite a construção de uma RAN com módulos de diferentes fornecedores. Para tratar da padronização da rede é preciso, antes, verificar a arquitetura *OpenRAN*.

[17] https://tinyurl.com/yh2ysk8w

4.2. Arquitetura e Interfaces

Há algumas instituições de padronização da *OpenRAN* mais proeminentes, como *Telecom Infra Project* (TIP), O-RAN *Alliance*, *Small Cell Forum*, *Open Networking Forum* e *Open* RAN *Policy Coalition* dentre outras. Como a O-RAN *Alliance* possui uma documentação bem detalhada[18], será utilizada como referência. Os elementos-chave dessa proposta são:

- *Service Management and Orchestration Framework* (SMO)
- RAN *Intelligent Controller* (RIC)
- *OpenCloud*
- *OpenRAN Central Unit* (O-CU)
- *OpenRAN Distributed Unit* (O-DU)
- *OpenRAN Radio Unit* (O-RU)

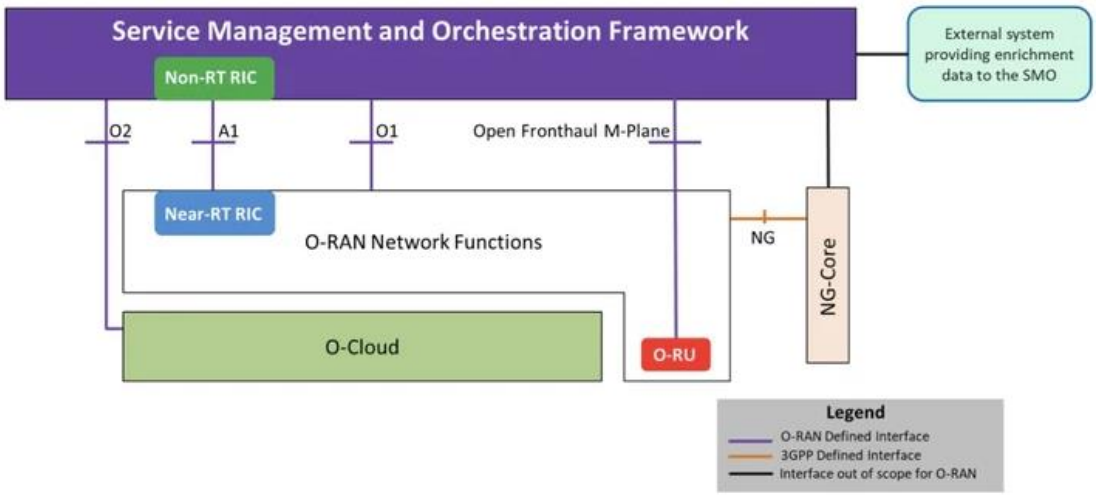

Figura 1 – Arquitetura *OpenRAN* (https://tinyurl.com/yjy4ao4e)

A Figura 1 – Arquitetura *OpenRAN* (https://tinyurl.com/yjy4ao4e) mostra as várias interfaces abertas que conectam a *OpenCloud*, as funções de rede *OpenRAN*, a unidade de rádio (RU), os controladores inteligentes de rádio (RIC's) e o núcleo de rede de próxima geração (NG-*Core*).

As definições dos elementos da Arquitetura *OpenRAN* vêm de https://tinyurl.com/yhr4z6pb:

O SMO inclui uma malha de integração e serviços de dados para as funções que gerencia. A malha permite que funções gerenciadas interoperem e se comuniquem dentro da *OpenRAN*. O SMO se conecta e gerencia os RIC's, *OpenCloud*, O-CU e O-DU.

[18] https://tinyurl.com/yfe79wwv

Existem dois tipos de RIC's: tempo não real e tempo quase real. Ambos são funções lógicas para controlar e otimizar os elementos e recursos de uma *OpenRAN*. Um RIC em tempo quase real controla e otimiza mais especificamente elementos e recursos com coleta de dados granulares e comunicação pela interface E2. A interface E2 conecta o RIC em tempo quase real com o O-CU e O-DU.

Um RIC em tempo não real usa inteligência artificial e aprendizado de máquina que incluem treinamento de modelo, onde os fluxos de trabalho aprendem como controlar e otimizar os elementos e recursos RAN.

O *OpenCloud* é uma plataforma de computação em nuvem composta por nós de infraestrutura física usando a arquitetura *OpenRAN*. Ele também cria e hospeda as várias funções de rede virtual (VNFs) usadas pelos RIC's e outros elementos de infraestrutura.

O O-CU é outro nó lógico que hospeda protocolos, que são o controle de recursos de rádio (RRC), protocolo de adaptação de dados de serviço (SDAP) e protocolo de convergência de dados de pacote (PDCP). O O-CU possui dois elementos distintos para gerenciar esses diferentes protocolos; o plano de controle O-CU hospeda o RRC e a parte do plano de controle do PDCP. A parte do plano do usuário hospeda o SDAP e a parte do plano do usuário do PDCP.

O O-DU também é um nó lógico, mas que hospeda outro conjunto de protocolos, que são o protocolo de controle de link de rádio (RLC), o protocolo de controle de acesso ao meio (MAC) e a interface física (PHY). O O-DU usa o protocolo PHY para se comunicar com a camada física da rede.

Finalmente, o O-RU processa radiofrequências recebidas pela camada física da rede. As frequências de rádio processadas são enviadas ao O-DU por meio de uma interface *fronthaul*. O O-RU é o único elemento da arquitetura da O-RAN Alliance não gerenciado pelo SMO. Em vez disso, ele é gerenciado pelo O-DU.

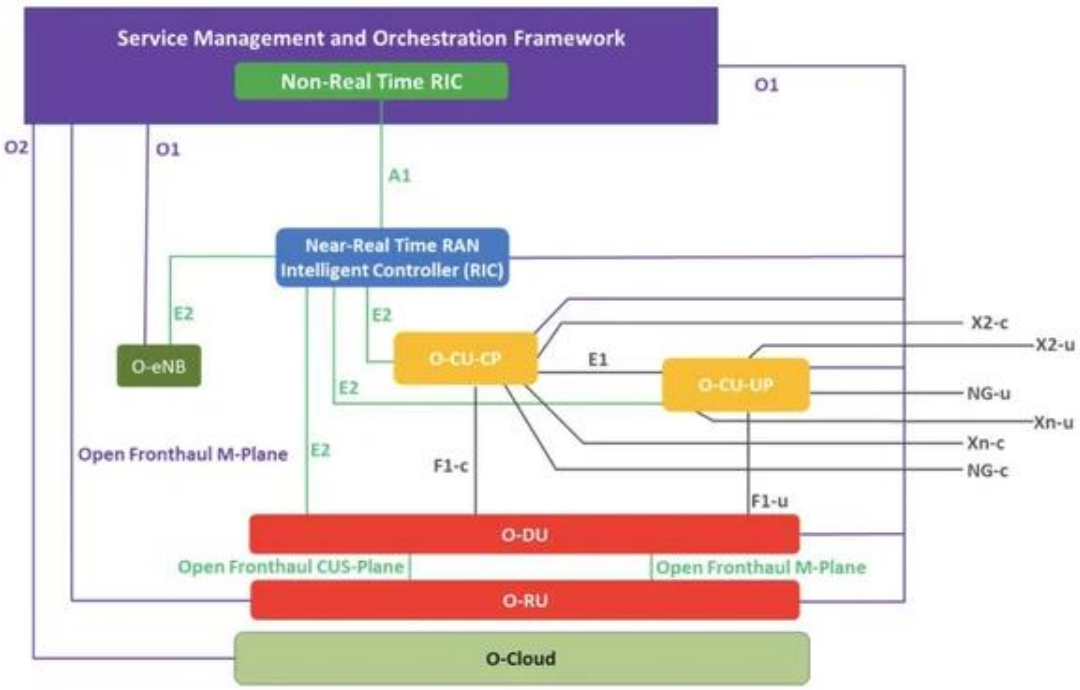

Figura 2 – Interfaces da arquitetura *OpenRAN* (https://tinyurl.com/yjy4ao4e)

Já de https://tinyurl.com/yfe79wwv é possível ver o detalhamento das interfaces da arquitetura *OpenRAN*:

A Interface *fronthaul* aberta conecta o O-DU e a unidade de rádio aberta (O-RU). Ela se divide no plano de gerenciamento (M-*Plane*) e no plano de sincronização, usuário e controle (CUS-*Plane*). O M-*Plane* conecta o O-RU ao O-DU e pode conectar o O-RU ao SMO. O O-DU usa o M-*Plane* para gerenciar o O-RU, enquanto o SMO pode fornecer serviços FCAPS (acrônimo para falha, configuração, contabilidade, desempenho, segurança) para o O-RU.

O CUS-*Plane* é multifuncional. Os aspectos de controle e de usuário transferem sinais de controle e dados de usuário, respectivamente. O aspecto restante sincroniza atividades entre vários dispositivos RAN.

A interface A1 permite a comunicação entre os dois RIC's e oferece suporte ao gerenciamento de políticas, transferência de dados e gerenciamento de aprendizado de máquina. Os dados, na verdade chamados de *enrichment information* (informações de enriquecimento), são especificamente para auxiliar no treinamento do modelo para IA e aprendizado de máquina no RIC quase em tempo real.

A interface O1 conecta o SMO aos elementos gerenciados por RAN. Estes incluem o RIC quase em tempo real, O-CU, O-DU, O-RU e o *NodeB* evoluído aberto (O-eNB). O O-eNB é o aspecto de *hardware* de um RAN 4G. As funções de gerenciamento e orquestração são recebidas pelos elementos gerenciados por meio da interface O1. O SMO, por sua vez, recebe dados dos elementos gerenciados por meio da interface O1 para o treinamento do modelo de IA.

A interface O2 é a conexão que permite ao SMO se comunicar com a *O-Cloud* em que reside. Os operadores de rede que estão conectados à *O-Cloud* podem operar e manter a

rede com as interfaces O1 ou O2 reconfigurando os elementos da rede, atualizando o sistema ou atualizar o sistema.

A interface X2 é dividida nas interfaces X2-c e X2-u, onde a primeira é para o plano de controle e a última é para o plano do usuário. Ambas são originalmente projetadas pelo 3GPP (*3rd Generation Partnership Project* é uma organização de telecomunicações para padronizar arquivos multimídia em telefones celulares e outros aparelhos wireless) para enviar informações entre eNB's de uma rede 4G, ou entre um eNB e um en-gNB de rede 5G. Na documentação da O-RAN *Alliance*, a interface tem os mesmos princípios e protocolos. Na Figura 2, ambas as interfaces X2 vêm de fora da arquitetura, mostrando que estão entrando em outra implantação. As interfaces Xn, NG, F1 e E1 também são adotadas a partir dos padrões 3GPP.

A interface Xn também é dividida em subtipos de controle e de usuário - Xn-c e Xn-u. Eles transferem o controle e as informações do plano do usuário entre os *NodeB's* de próxima geração (gNB's), entre os ng-eNB's (nós 4G capazes de se conectar a um núcleo 5G) ou entre os dois tipos diferentes.

O controle NG e as interfaces do plano do usuário conectam um plano de controle da O-CU (O-CU-CP) e o plano do usuário da O-CU (O-CU-UP) ao núcleo 5G. As informações do plano de controle vão para a função de gerenciamento de mobilidade e acesso 5G (AMF), que recebe informações de conexão e sessão do equipamento do usuário. As informações do plano do usuário vão para a função do plano do usuário 5G (UPF), que lida com muitos aspectos de roteamento, encaminhamento e tunelamento.

A interface F1, novamente dividida em subtipos de plano de controle e usuário, conecta o O-CU-CP e O-CU-UP ao O-DU. Ele troca dados sobre o compartilhamento de recursos de frequência e outros status da rede. Um O-CU pode se comunicar com vários O-DU por meio de interfaces F1.

A última das interfaces baseadas em 3GPP é a interface E1. Ela conecta o O-CU-CP e o O-CU-UP. Ela transfere dados de configuração e informações de capacidade entre os dois planos O-CU. Os dados de configuração garantem que os dois planos possam interoperar. As informações de capacidade são enviadas do plano do usuário para o plano de controle e incluem o status do plano do usuário.

O RIC quase em tempo real na arquitetura RAN aberta se conecta ao O-CU, O-DU e O-eNB com a interface E2. Esses elementos combinados formam o nó E2. Um nó E2 só pode se conectar a um RIC quase em tempo real, mas um desses RIC's pode se conectar a vários nós E2. Os protocolos que passam pela interface E2 são apenas protocolos de plano de controle. Os protocolos são para controlar e otimizar os elementos do nó E2 e os recursos que eles usam. Novamente, os dados coletados são retornados ao RIC pela interface.

Verificando, então, os detalhes da arquitetura *OpenRAN*, pode-se afirmar que:

- A sua padronização inclui trabalho em controladores de rede, estruturas de gerenciamento e interfaces que conectam todos os elementos de rede na infraestrutura de rede.

- Os RIC's automatizam a rede.
- Há uma infinidade de interfaces em funcionamento conectando as várias partes da infraestrutura *OpenRAN*, algumas das quais são emprestadas dos padrões 3GPP.

Os principais órgãos de padronização para RAN aberta são a O-RAN *Alliance*, o *Telecom Infra Project*, *Open RAN Policy Coalition* e *Open Networking Forum*, dentre outros.

4.3. Topologias e *splits*

As redes abertas de acesso rádio oferecem a opção de colocar funções de rede em diferentes locais ao longo do caminho do sinal. Essa opção, chamada de *split* funcional, permite que haja otimização de desempenho e adaptações para montagem de diferentes topologias de redes.

Historicamente, as arquiteturas de rede de acesso rádio (RAN) foram baseadas em blocos de construção monolíticos. Essas redes, que cruzam as diferentes gerações de comunicações móveis, continham suas funções nas unidades de banda base (BBUs) na base das torres de rádio. As BBUs demodulam o sinal de RF, convertendo a saída em fluxos de dados digitais para transporte no *backhaul* para a rede central. Com o advento de redes abertas, esta situação está mudando.

Desde as primeiras fases do 5G *New Radio* (NR), tem havido um esforço para desagregar a BBU dividindo suas funções antes presentes na Unidade de Rádio (RU) em Unidades Distribuídas (DUs) e Unidades Centralizadas (CUs). O argumento para a desagregação era a flexibilidade, permitindo que as operadoras de rede decidissem como localizar essas funções e maximizar o desempenho. As implementações de *hardware* e *software* flexíveis permitem implantações de rede escalonáveis e econômicas. Para que a desagregação aconteça, os componentes de *hardware* e *software* devem ser interoperáveis, permitindo que os engenheiros de rede misturem e combinem essas unidades de diferentes fornecedores. A desagregação também traz vantagens e desvantagens na decisão de qual unidade deve controlar certas operações – a *split* funcional.

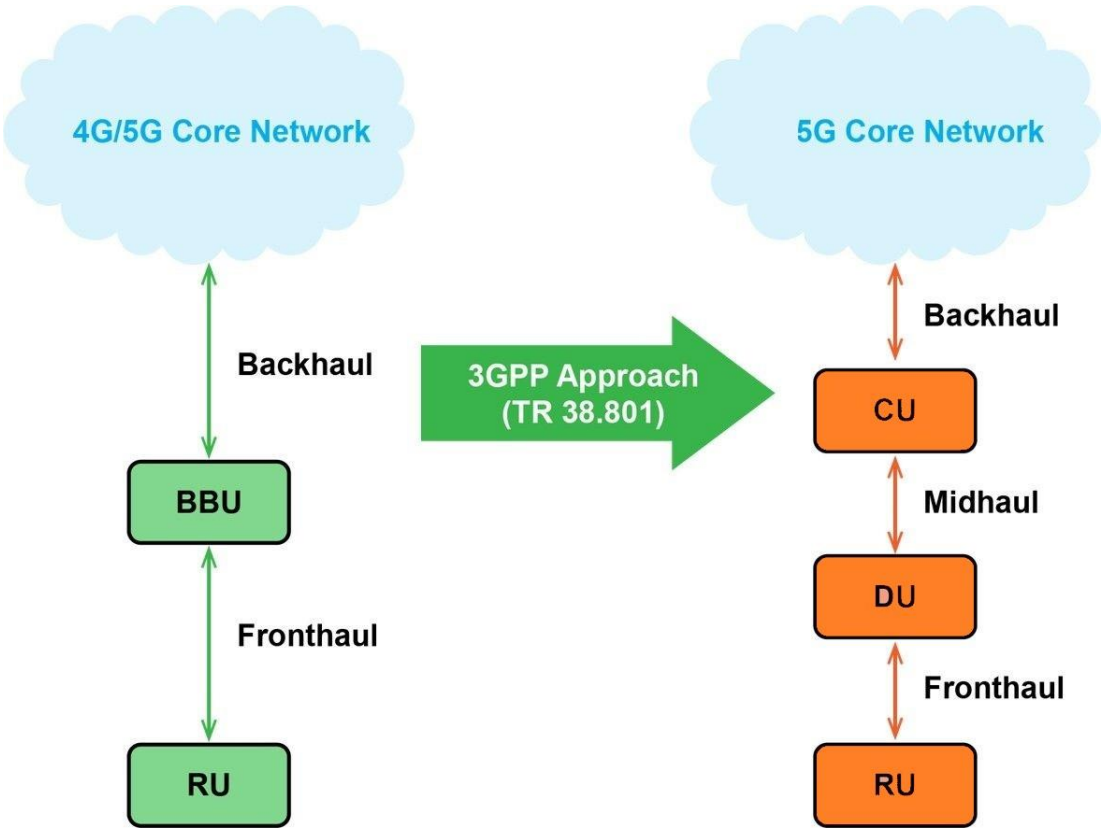

Figura 3 – Segregação da BBU (https://tinyurl.com/yhx9xf8y)

Como a *split* de RAN é totalmente virtualizada, as funções de CU e DU são executadas como funções de *software* virtual em *hardware* comercial (COTS, *Commercial off-the-shelf*) e podem ser implantadas em qualquer *data center*.

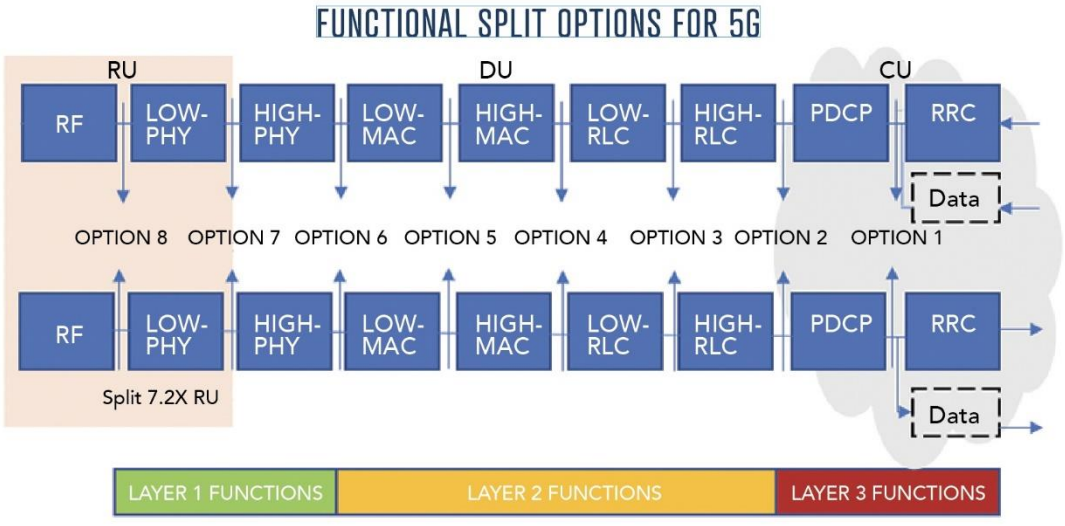

Figura 4 – Opções de *splits* (https://tinyurl.com/yhx9xf8y)

Ao centralizar totalmente as funcionalidades da RAN, a opção 8 coloca as mais altas demandas no *fronthaul*, com altas taxas de bits e requisitos de latência estritos. Do outro lado, a *split* 1 coloca todo o processamento de banda base dentro da RU, que se torna grande, complexa e requer mais energia do que a RU simplificada da opção 8. As

demandas de *fronthaul* da *split* 8 são, no entanto, muito mais simples porque toda a pilha de protocolos reside na RU. Isso significa que mais processamento deve ocorrer antes que os dados possam viajar entre RU e CU, levando a taxas de bits muito mais baixas e tolerâncias de latência mais altas no *fronthaul*. As opções de *split* restantes, de 2 a 7, variam no nível de processamento de banda base restante na RU em oposição a ser hospedado na DU e na CU. Quanto maior o índice da *split*, menores serão as demandas no link do *fronthaul*, equilibradas contra os benefícios decrescentes da centralização.

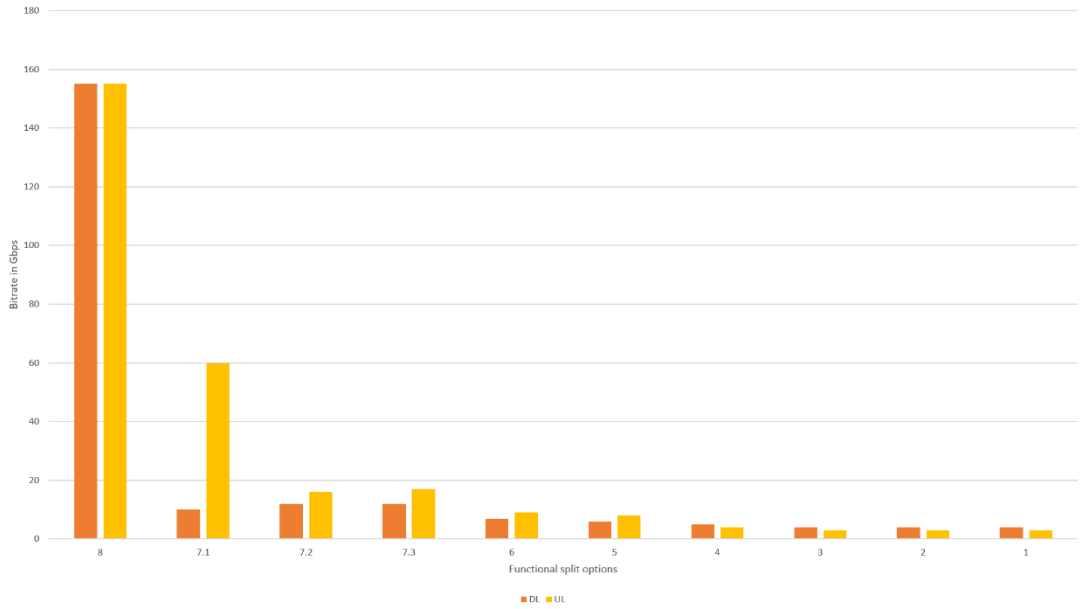

Figura 5 – Taxa de bits no *fronthaul* vs. *splits* (https://ieeexplore.ieee.org/document/8479363)

Não existe uma *split* ideal porque diferentes opções se adequarão a diferentes aplicações. É, no entanto, improvável que a indústria pudesse apoiar todas as oito opções. Para garantir escala e abertura, várias alianças do setor estão trabalhando para obter consenso sobre as melhores opções a serem adotadas. O 3GPP recomenda a opção 2 para aplicações centralizadas, como acesso sem fio fixo (FWA), onde a coordenação do local da célula não é necessária e os requisitos de latência e largura de banda na rede de transporte são menos exigentes.

Ao mesmo tempo, a opção 6 está sendo promovida pelo *Small Cell Forum* (SCF), como a divisão ideal para implantações de baixo custo e baixa capacidade. O SCF desenvolveu especificações para essa *split* conhecida como nFAPI, (interface de programação de aplicação funcional de rede).

Por fim, a O-RAN *Alliance* oferece suporte à opção 7.2 para redes com requisitos de alta capacidade e confiabilidade. Essa *split* funcional permite uma RU relativamente simples, cujo tamanho e consumo de energia suportam a densificação da rede e permitem o compartilhamento por várias operadoras, facilitando o desenvolvimento do mercado de redes neutras. A capacidade da eCPRI de funcionar em Ethernet é uma vantagem significativa em áreas urbanas e em ambientes internos, como Indústria 4.0 e blocos de escritórios, onde a cobertura 5G será necessária.

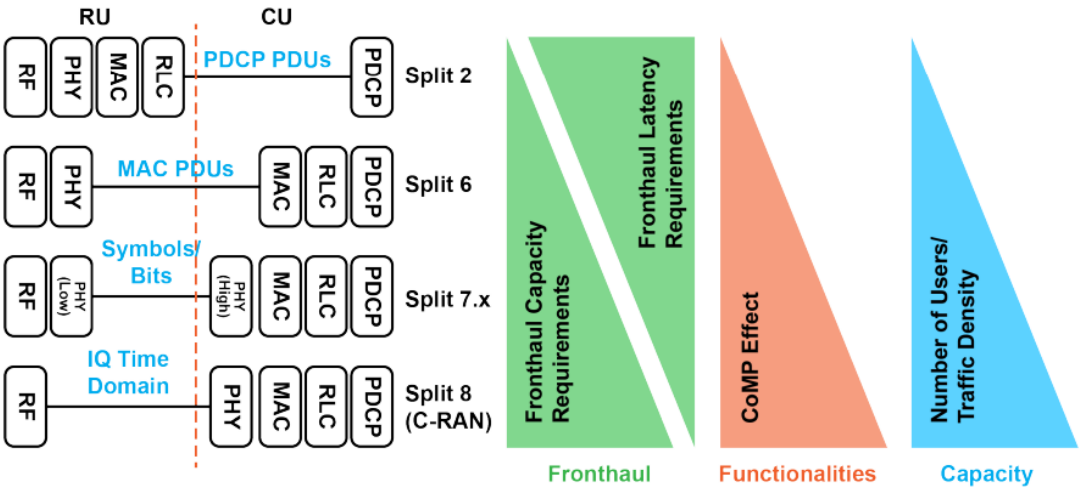

Figura 6 – *Tradeoff* para diferentes *splits* (https://tinyurl.com/yhluuug2)

> *CPRI (*Common Public Radio Interface*, Interface Pública Comum de Rádio) é uma interface que envia dados das RRUs para a unidade de banda base. É serial com uma conexão de alta velocidade. Mas à medida que se avança para 5G, a fibra entre as RRUs e a unidade de banda base vai transportar muito mais tráfego, e isso torna mais difícil fazer uma interface serial. Desta forma surge a eCPRI (*enhanced *CPRI, CPRI melhorada), que é uma maneira de dividir as funções da banda base e colocar parte dessa funcionalidade na RRU para reduzir a carga sobre a fibra. Salienta-se que a eCPRI, diferentemente da CPRI, é uma interface aberta.*

4.3.1. *Splits* mais recomendadas

A escolha adequada de *splits* permite o melhor aproveitamento das tecnologias importantes à RAN, em especial *carrier aggregation* e *advanced* RAN *coordination*, salientando o objetivo geral de otimização de cobertura, capacidade e latência. Outro ponto importante é que a interface eCPRI permite a quebra dinâmica de funções na RAN.

As opções de índices mais altos de *splits* demandam baixa banda e atraso no transporte menor do que 75 µs. Já as opções mais baixas permitem melhores coordenação e escalonamento conjunto de aplicações de mobilidade, permitindo o *interworking*.

Split 2: Divisão RRC / PDCP. O controle de recursos de rádio e o controle de convergência de pacotes de dados são separados do controle de enlace de rádio da camada 2 (RLC). Como explicitado antes, o 3GPP recomenda a opção 2 para aplicações centralizadas, que pode ser implantada em duas variantes:

- Variante 1: RRC, protocolo de adaptação de dados de serviço (SDAP) e PDCP na mesma unidade central de uma entidade; nenhum controle e divisão de usuário. O RLC, o controle de acesso ao meio (MAC) e a camada física alta

(*High* PHY) farão parte do DU, e a camada física baixa (*Low* PHY) junto com o RF estão no RU.

- Variante 2: Além da Variante 1, esta *split* vem com controle e divisão de usuário como em um CU-CP e CU-UP. O RRC junto com o PDCP-C fará parte do CU-CP e o SDAP / PDCP-U será associado ao CU-UP.

A *split* 2, que se adequa, por exemplo, a acesso fixo sem fio, permite inserir mais funções no rádio, agregando RU e DU, relaxando o requisito de atraso sobre transporte, sendo possível estender o *fronthaul* em quilômetros e economizar banda, sendo aplicável, por exemplo, em redes rurais.

Os casos de uso ideais da *split* 2 incluem cenários onde uma baixa taxa de bits é necessária para ser transportada por um *fronthaul* menos ideal, onde maior segurança e resiliência são obtidas pela separação entre plano de controle e plano de usuário. Suas vantagens mais importantes são criptografia e integridade centralizada e coordenação aprimorada de procedimentos de mobilidade e transferência de sessão. Esta divisão traz o PDCP centralizado no plano de usuário, que pode ser separado do RRC / RRM no plano de controle, portanto, é altamente tolerante à latência. Permite ganhos de *beamforming*, embora não tenha coordenação eficiente entre várias DUs, ou seja, a coordenação não é rápida o suficiente para aplicativos de baixa latência. Oferece apenas ganhos marginais de multiplexação no *pool* de CU porque a maioria das funções críticas está na DU, que pode ser parte da implantação do *site* ou próximo à célula, como em um *data center* local.

Split 6: Divisão da camada MAC / PHY. O MAC, RLC e camadas superiores farão parte da unidade central (CU). Não há divisão *Low* PHY / *High* PHY; em vez disso, a pilha completa da camada PHY e RF estão no DU / RU. A interface nFAPI na *split* 6 permite que qualquer CU / DU *Small Cell* se conecte a qualquer unidade de rádio *Small Cell* (S-RU).

A *split* 6 é mais adequada para implantação de *small cells* tipo *femtocell*, bem como onde *backhaul* e *fronthaul* heterogêneos com desempenho variável estão disponíveis e são necessários para atender a diferentes *small cells*. Em comparação com a *split* 7,2x, a opção 6 mostra desempenho inferior em *cell-edge user throughput* e *average cell throughput*. Vem com redução significativa da largura de banda do *fronthaul* em comparação com a opção 7,2x.

Split 7.2x: A divisão *Low* PHY / *High* PHY é a abordagem mais comum, pois é menos complexa e oferece suporte a vários requisitos de *fronthaul* e, o mais importante, tem altos benefícios de virtualização. Essa *split* foi otimizada pela O-RAN *Alliance* em duas variantes: *split* 7.2a e *split* 7.2b. A *split* 7.2x vem com técnicas de compressão de *fronthaul* para reduzir ainda mais a largura de banda de transporte. No caso de requisitos para serviços mais sensíveis a atrasos, com base na disponibilidade de *fronthaul* apropriada, a divisão MAC-PHY será a solução preferida, como em áreas densas e urbanas. A camada física possui aplicações que exigem muitos recursos, a deixando pesada. Assim, a *split* 7.2, como as demais subopções 7, reduz a banda necessária para transporte, sendo aplicável a *Massive* MIMO (*multiple-input and multiple-output*, Múltiplas Entradas e Múltiplas Saídas).

A *split* 7.2 se aplica em situações em que um *fronthaul* ideal é possível para URLLC (*Ultra-Reliable Low-Latency Communication*, Comunicação Ultra Confiável de Baixa Latência) e *carrier aggregation*, com presença de eCPRI para implantação com *data centers* locais virtualizados. Ela oferece suporte a casos de uso em que a utilização eficiente de recursos de multi-RAT e multi-conectividade é necessária. Suporta "multi-TRP", recepção conjunta, agregação de múltiplas operadoras e recursos semelhantes que precisam de baixa latência. A principal restrição nesta abordagem é o requisito rigoroso de alta latência por causa das interações de temporização no *subframe* entre parte da camada PHY na CU e parte da camada PHY nas DUs. O *fronthaul* precisa atender a certas QoS para garantir a prioridade para dados críticos de tempo.

Split 8: Divisão PHY-RF. Esta divisão definida pelo 3GPP foi considerada anteriormente em *designs* tradicionais baseados em C-RAN, incluindo CPRI que suporta RRUs, mas ainda oferece benefícios para 5G em alguns casos específicos. Essa divisão permite a separação completa da RF da camada física para ganhos máximos de virtualização. Tudo, desde a camada física até a camada superior, incluindo todos os níveis da camada de protocolo, é centralizado, resultando em uma RAN fortemente coordenada. Isso permite o suporte eficiente de recursos 5G avançados que exigem latência extremamente baixa, como transmissão e recepção de TRP múltiplo, MIMO de alta ordem e alta diversidade para tráfego semelhante a URLLC. A *split* 8 é altamente eficaz em 2G e 3G, onde as taxas de tráfego são mais baixas e, portanto, o processamento em si, a princípio, é mais baixo e pode ser feito facilmente em um servidor x86, permitindo que as operadoras usem RUs com custo otimizado com o mínimo processamento.

Já para aplicações que demandam baixíssimo atraso, tais como mMTC (*massive Machine-Type Communications*, Comunicações maciças do Tipo Máquina) e URLLC, o que envolve redes com aplicações IoT e Indústria 4.0, pode-se utilizar *Double Split*, combinando-se uma *split* de mais baixa ordem com outra mais alta e, assim, garantir com que o *backhaul* tenha atraso de 1 a 10 ms.

4.3.2. Topologias

Com as diferentes *splits* possíveis, é possível às operadoras montarem suas redes de diversas formas, considerando diferentes necessidades. Um dos aspectos relevantes ao se projetar uma rede é o *tradeoff* entre transporte e localização. Uma maneira de se verificar qual topologia se enquadra em cada necessidade é comparar o TCO (*Total Cost of Ownership*, Custo Total de Propriedade) em redes com diferentes custos de transporte. Para a comparação das diferentes topologias, serão considerados três cenários[19]:

- Cenário 1 – topologia distribuída. DU e RU remotos ligadas à CU pelo *midhaul*;
- Cenário 2 – topologia parcialmente distribuída. As três unidades segregadas;

[19] "*OpenRAN: Which OpenRAN is best for you?*" Copyright © 2021 Mavenir, Inc. and Senza Fili Consulting LLC. All rights reserved.

- Cenário 3 – topologia centralizada. DU e CU no *data center* conectadas à RU pelo *fronthaul*.

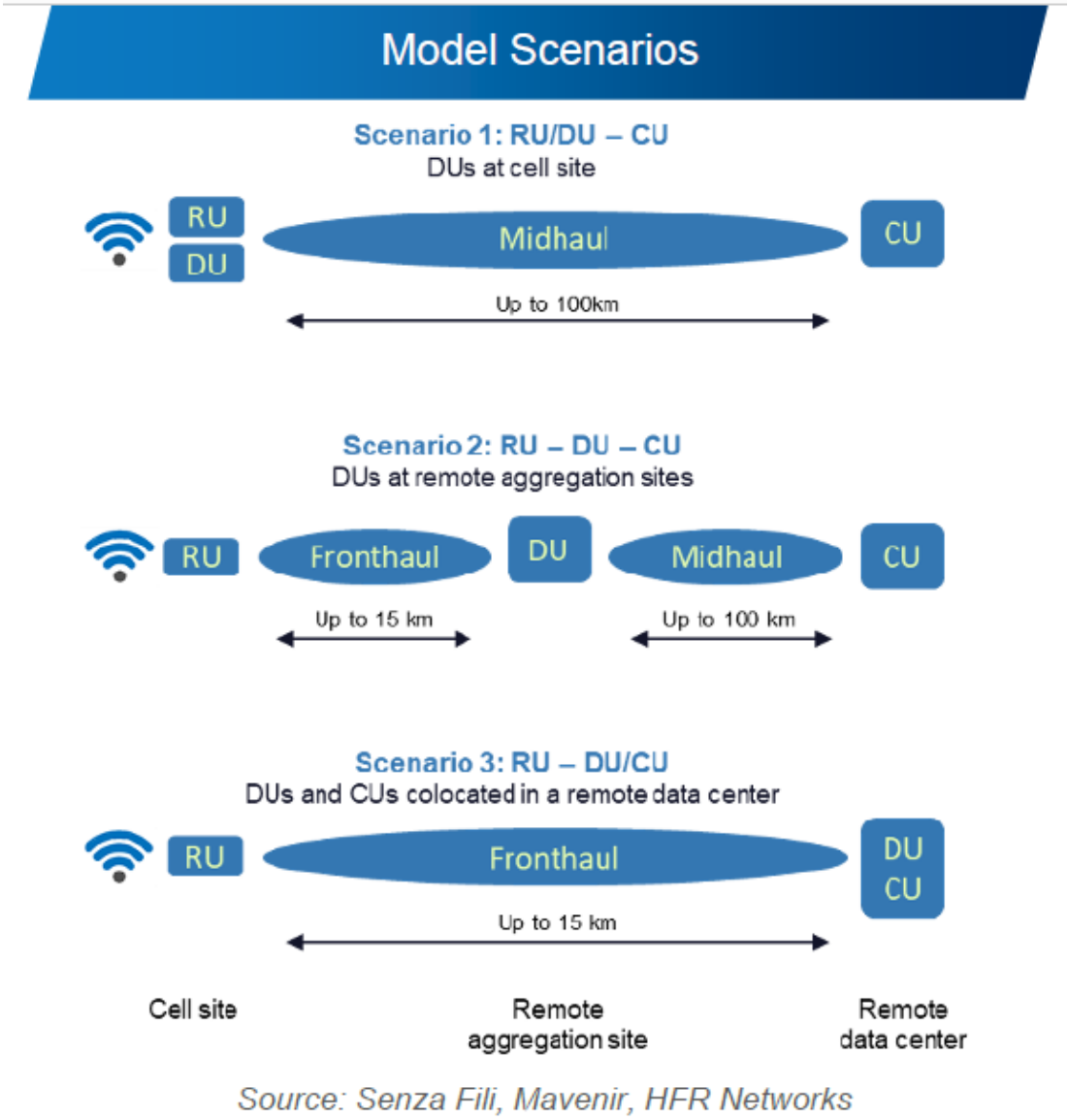

Figura 7 – Topologias possíveis

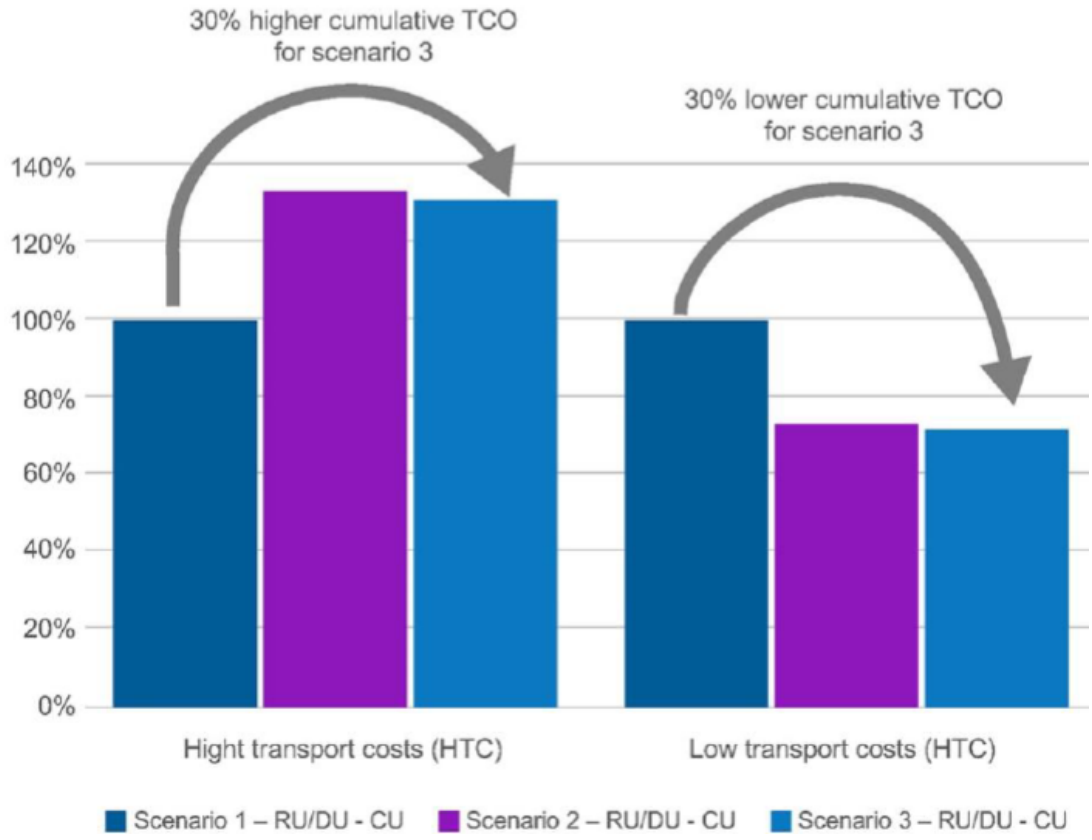

Figura 8 – TCO vs. custos de transporte

Com *OpenRAN*, as operadoras, ou redes, com HTC (*High Transport Costs*, Altos Custos de Transporte) podem economizar 30% em 5 anos, se usarem uma topologia distribuída com a DU no local da célula, em vez de uma topologia centralizada com DU e CU em locais remotos. Para operadoras, ou redes, com LTC (*Low Transport Costs*, Baixos Custos de Transporte) uma topologia centralizada pode economizar 30% comparando com uma topologia distribuída.

É mais provável que HTC se aplique a uma operadora móvel *brownfield* que não possui a rede de transporte e tem que pagar preços de mercado por ela. O caso LTC é mais típico de uma operadora que possui uma rede de transporte e, portanto, baixo custo com essa parte da infraestrutura. Como a única diferença entre HTC e LTC é o custo de transporte, o TCO para o caso HTC é maior.

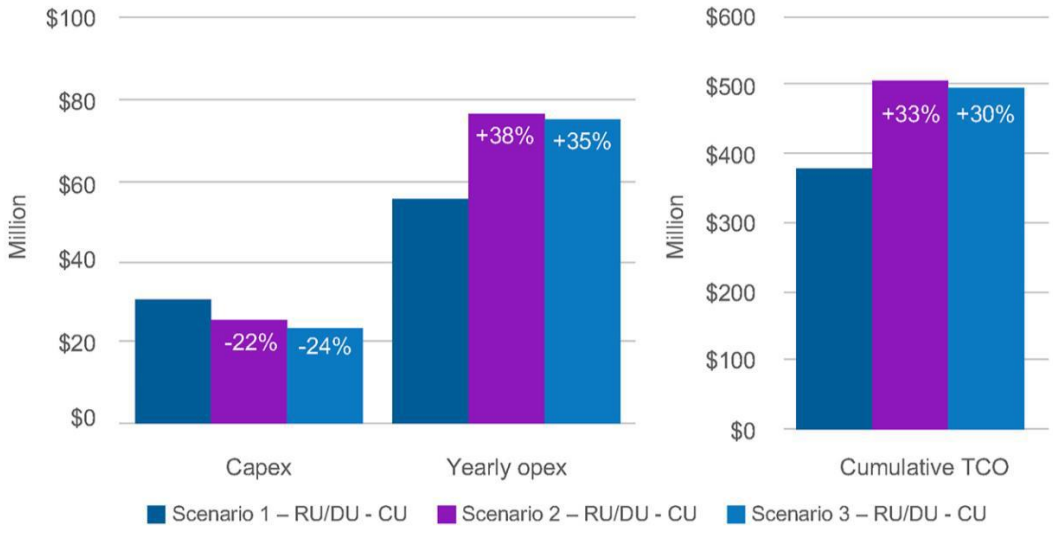

Figura 9 – Capex, Opex e TCO vs. custos de transporte para HTC

Para o caso HTC (Figura 9 – Capex, Opex e TCO vs. custos de transporte para HTC), os custos mais altos de instalação de mais equipamentos nas estações de células dão ao cenário 1 o maior Capex (*Capital Expenditure*, Despesas de Capital). No entanto, os requisitos de transporte mais baixos no cenário 1 reduzem o Opex (*Operational Expenditure*, Despesas Operacionais) geral em comparação com os cenários 2 e 3.

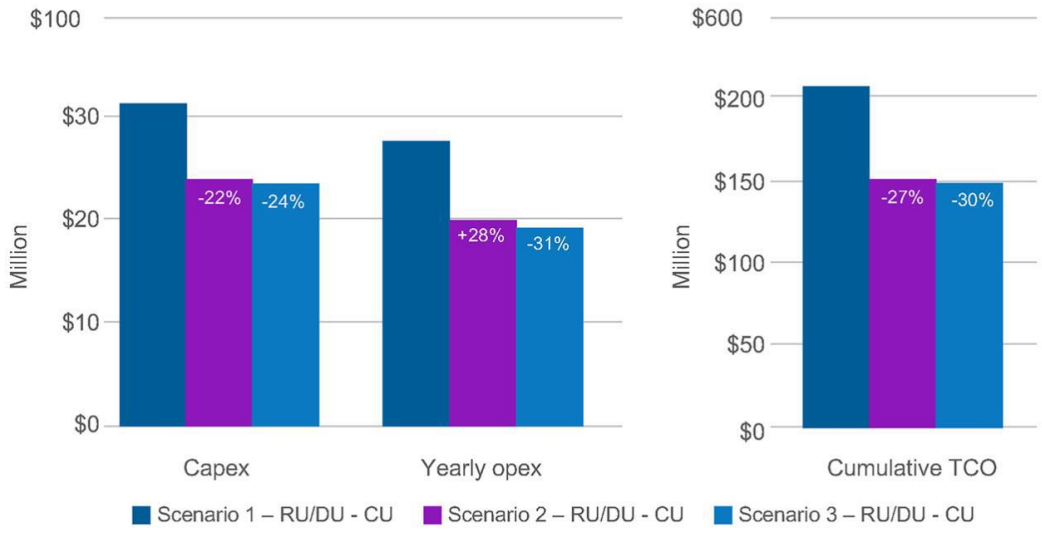

Figura 10 – Capex, Opex e TCO vs. custos de transporte para LTC

Para a situação LTC, as diferenças percentuais no Capex entre os cenários são as mesmas do caso HTC. Como no HTC, um custo de equipamento de local de célula mais baixo favorece os cenários centralizados 2 e 3. Os custos de transporte mais baixos impulsionam a maior parte da redução de Opex. Economias adicionais em Opex vêm do menor custo de concentração do Capex de DU e CU em locais remotos.

4.3.3. *OpenRAN* e soluções customizadas

Identificando corretamente a melhor topologia para alguma aplicação específica, é possível alcançar parâmetros até melhores do que encontrados em redes monolíticas. Alguns KPIs[20] alcançados em redes já instaladas, considerando diferentes tecnologias como 4G LTE (*Long Term Evolution*, Evolução a Longo Prazo; no Brasil, é a tecnologia adotada em redes 4G), 5G, TDD, FDD, e em diferentes aplicações como subúrbios, áreas densas, áreas rurais, indústria e outras são mostrados a seguir:

- LTE *call setup* 99,3%
- VoLTE[21] *call setup* 99,5%
- CSFB 100%
- HO *success rate* 99%
- *Downlink throughput* @ 15 MHz 90Mbps
- *Uplink throughput* @ 15 MHz 40Mbps
- LTE *call drops* 0,17%
- VoLTE *call drops* 0,3%

a) Cenário 1

A agregação da RU com a DU, mantendo a CU em um ponto remoto, permite a conexão destes dois pontos através do *midhaul* em até 100 km. Compatível com a *split* 2, este cenário pode ser aplicado onde se encontra um *fronthaul* menos ideal, onde maior segurança e resiliência são obtidas pela separação entre plano de controle e plano de usuário. Suas vantagens mais importantes são criptografia e integridade centralizada e coordenação aprimorada de procedimentos de mobilidade e transferência de sessão. Como já detalhado, tem aplicações especialmente em áreas rurais, o que para operadoras que precisam contratar redes de transporte de terceiros, pode representar economia de até 30% de TCO. Este cenário poderia ser favorável a expansão da rede em *greenfield* por ISP's (*Internet Service Providers*, Provedoras de Internet), PPP's (Prestadoras de Pequeno Porte) e operadores de redes neutras.

Estima-se que o cenário 1 para o caso HTC traz economias de Opex da ordem de 30%, reforçando sua aptidão para redes *greenfield*, por mais que o Capex para esta situação seja menos favorável.

b) Cenário 2

A segregação dos três elementos de rede, RU, DU e CU em *sites* diferentes é compatível com *double split*, ou seja, a utilização de uma *split* de ordem mais baixa com uma de ordem mais alta. É um cenário favorável a PMS's (operadoras detentoras de

[20] *Open RAN Summit*, em https://onlinexperiences.com/Launch/Event.htm?ShowKey=163825
[21] *Voice over* LTE, Voz sobre LTE

poder de mercado significativo) que possuem sua rede de transporte bem estabelecida no *brownfield* e em aplicações em que a latência é um KPI essencial. Assim como no cenário 3, sua aplicação permite reduções de TCO da ordem de 30% para operadoras com baixo custo de transporte. Ambientes que podem se aproveitar deste cenário são Indústria 4.0 e zonas urbanas densas.

Conforme Figura 9 – Capex, Opex e TCO vs. custos de transporte para HTC e Figura 10 – Capex, Opex e TCO vs. custos de transporte para LTC, percebe-se que os benefícios de Capex e Opex se estendem para o caso LTC quando aplicado ao cenário 2, reforçando a predisposição desta topologia a regiões com grande adensamento.

c) Cenário 3

A *split* 7.2, conforme explicitado no item *Splits* mais recomendadas, reduz a banda necessária para transporte, sendo aplicável a *Massive* MIMO e URLLC, o que permite utilização com baixa latência, como na indústria 4.0 e redes privativas, compatíveis com o cenário 3 da Figura 7 – Topologias possíveis Nesta montagem, a distribuição de interfaces, containerização e virtualização permite economias na ordem de 40% de TCO em cinco anos sobre RU, DU e CU[22]. Esta topologia é compatível com atualizações de redes das PMS's em suas áreas mais densas.

Também se valendo deste cenário as PMS's podem formatar redes *small cell* por meio da *split* 6, da mesma maneira alcançando economias de TCO de cerca de 40%.

Do ponto de vista de Capex, o cenário 3 tem vantagem de economia da ordem de 20%, seja para prestadoras com baixos ou altos custos de transporte, porém para Opex esse benefício se mantém para o caso LTC, reforçando sua consagração para redes *brownfield*, conforme Figura 9 – Capex, Opex e TCO vs. custos de transporte para HTC e Figura 10 – Capex, Opex e TCO vs. custos de transporte para LTC

5. ETAPA 1 – MAPEAMENTO

Na etapa de mapeamento, o foco recai na imersão sobre as temáticas nucleares do projeto, com vistas ao delineamento conceitual, à consciência situacional e à compreensão dos elementos constituintes do problema de pesquisa. Inicia-se abrangendo a definição do problema em si, a fundamentação teórico-conceitual, as expectativas das partes interessadas, as outras soluções tecnológicas já disponíveis e as implicações do *OpenRAN* para a indústria e o mercado de telecomunicações.

Esse processo de descoberta de conhecimento é realizado por meio da imersão aos eixos temáticos, identificando várias perspectivas presentes e situações particulares que fazem parte dos diferentes contextos e domínios que se encerram na implementação do *OpenRAN*.

[22] *Open RAN Solutions Showcase – Day* 2, em https://www.youtube.com/watch?v=fOllo44j8mA&t=13055s

Ao longo do mapeamento, as equipes de pesquisadores se aproximam do domínio do problema e esclarecem os eixos temáticos, além de dimensionar o alcance das linhas de base das pesquisas. Inicia-se com pesquisas e levantamento de artefatos de informação básicos sobre os eixos temáticos.

Por fim, as equipes de pesquisa ampliam os horizontes de estudo para poder explorar os contextos histórico, tecnológico, regulatório e mercadológico. Visa, portanto, encontrar todos os pontos de partidas que podem gerar insights para a continuidade do projeto de pesquisa básica em curso.

5.1. TED

Nesse sentido, a CEATEL elaborou termo de execução descentralizada com a Universidade de Brasília para que se analise academicamente e consolide os avanços sobre o *OpenRAN* em dez estudos que perpassam os eixos tecnológico, econômico e regulatório, que terá como vigência o prazo de 30 meses. Na seção CONCLUSÕES há um detalhamento maior sobre esta iniciativa.

5.2. GT *OpenRAN*

Em 31/03/2021 ocorreu a primeira reunião GT *OpenRAN* que tem por objetivo acompanhar os projetos de tal tecnologia no Brasil e propor eventuais ações regulatórias. O evento contou com mais de 100 participantes, dentre representantes do Ministério das Comunicações, da Anatel, prestadoras, fabricantes, laboratórios e associações representativas, sendo que muitos realizaram apresentações sobre as principais iniciativas que vêm desenvolvendo relativas à *OpenRAN*. Diante das apresentações realizadas na reunião inaugural, a equipe técnica da Anatel passou a ouvir os projetos de forma individualizada, sendo já realizados mais de 20 reuniões entre a Anatel, operadoras, laboratórios, universidades, institutos e fabricantes.

Em 16 de junho de 2021 realizou-se a segunda reunião do GT, onde se pontuou que neste momento deve-se priorizar autorregulação regulada, bem como o incentivo de aplicação de recursos de P&D em projetos afetos à *OpenRAN*.

5.3. Das reuniões do GT Técnico e projetos que serão acompanhados

Ocultado por informações técnicas de empresas (art. 39, § único, da lei nº 9472/1997).

5.4. Questões levantadas por *players* nas reuniões bilaterais

Entre as questões levantadas nas reuniões já realizadas, salienta-se:

A arquitetura *OpenRAN* ainda não está madura para utilização em larga escala. Os players estimam períodos diferentes para a maturação, em geral de dois a cinco anos. Entre os pontos críticos para o pleno desenvolvimento da arquitetura, foi mencionado o aumento da complexidade devido à desagregação, a falta de experiência das operadoras em integrar seus sistemas e a inexistência de RICs em pleno funcionamento e

automação. Além disso, há soluções com alto custo computacional e outras nem tanto, o que pode causar um descompasso no desenvolvimento da arquitetura. De qualquer maneira, orquestração e inteligência (ainda incipientes) no ambiente *OpenRAN* com compartilhamento de portadora talvez viabilize um RAN *sharing* mais intenso.

O dimensionamento de infraestrutura ainda é uma incógnita, com o foco direcionado em um primeiro momento a redes rurais e de baixa densidade.

A segurança da rede é um ponto controverso, pois alguns players afirmam que a abertura preconizada pela *OpenRAN* permitirá que as redes sejam mais fiscalizadas por mais entidades e fornecedores, já outros alegam que a virtualização permite uma maior superfície de ataque. Foi também salientado que a arquitetura aberta não oferece riscos diferentes de uma arquitetura tradicional, uma vez que os ataques em geral não são através da estrutura de telecomunicações da rede, mas sim da internet.

Outro ponto bastante discutido foi a necessidade de adequações ao modelo de certificação e homologação de equipamentos. Uma vertente levantada é a necessidade de se criar um selo *OpenRAN*, a fim de se garantir a interoperabilidade das redes. Outra é que não seria necessário alterações no modelo de certificação atualmente vigente, uma vez que entidades como ORAN *Alliance* e 3GPP estabelecem padrões que são respeitados pelos *players*. Salienta-se também que foi discutido a possibilidade de que a necessidade de se seguir padrões de entidades internacionais pode criar barreiras de entrada a novos *players*. Outras propostas envolviam certificação de *software* e de módulos que combinem *hardware* e *software* devido à desagregação entre eles. Possíveis atualizações poderiam alterar inclusive características de emissão radioelétrica.

Interoperabilidade e integração demandam segurança e pré-validação. Para isso, é necessário padronização, o que levaria também a redução de custos e garantia de atualizações durante a vida útil da rede, o que se reverte em qualidade na prestação do serviço. Essa padronização precisa ser estabelecida também entre RAN, core e dispositivos.

Expansão da rede atual por meio de soluções *Non Stand Alone* talvez cause inibição a adoção de soluções *OpenRAN Stand Alone* pois esta segunda pode não ter um desempenho tão bom a princípio, especialmente enquanto as redes abertas ainda não tiverem sido maturadas, fazendo com que as operadoras decidam por usar a primeira solução quando da expansão e atualização das redes previamente instaladas.

Por mais que haja a posição de alguns participantes do GT que não é necessário obrigações ou incentivos por parte do poder público para adoção da *OpenRAN* pelo mercado, houve manifestações para que haja políticas públicas de fomento para a tecnologia ser disseminada no país. Foi dito que os custos de importação de *hardware* são altos e que, por isso, seria interessante haver uma cadeia produtiva no país, o que hoje é difícil devido à competição com grandes fornecedores internacionais, sem contar que, hoje, o *hardware* COTS disponível para implantação de redes abertas não é barato e não suporta as demandas de rede que são suportadas por equipamento proprietário. Além deste ponto, citou-se a necessidade de capacitação de integradores nacionais devido a dificuldades de trabalhar com grandes fornecedores que focam em mercados

mais maduros. Quanto a *software*, os participantes do GT em geral entendem que o Brasil tem condições de fornecer as soluções necessárias.

Há membros do GT que entendem que a arquitetura *OpenRAN* deve focar na padronização de interfaces, o que seria suficiente para garantir uma maior competição entre fornecedores. Outros entendem que é necessário que a arquitetura seja realmente aberta, usando, por exemplo, softwares de código aberto.

Capacitação do corpo técnico, tanto das operadoras quanto das fornecedoras, demandará muito investimento, o que ainda não foi mensurado. A arquitetura de redes abertas quebra o paradigma da existência de um responsável por toda a estrutura, talvez sendo necessário maiores equipes para identificação e correção de falhas, por exemplo. Porém, a padronização tende a diminuir esses e outros custos.

Necessidade de associação a entidades de padronização *OpenRAN* poderia criar barreira para novos entrantes.

ORAN *Alliance* trabalhará na arquitetura *split* 7.2 – arquitetura de baixo nível (*low-level*) para comunicação ultra-confiável de baixa latência (*low-level split for ultra-reliable low-latency communication* – URLLC) e desenvolvimento *near-edge*, conforme Figura 11 – *Near-edge deployment* (https://tinyurl.com/yfhcjad6).

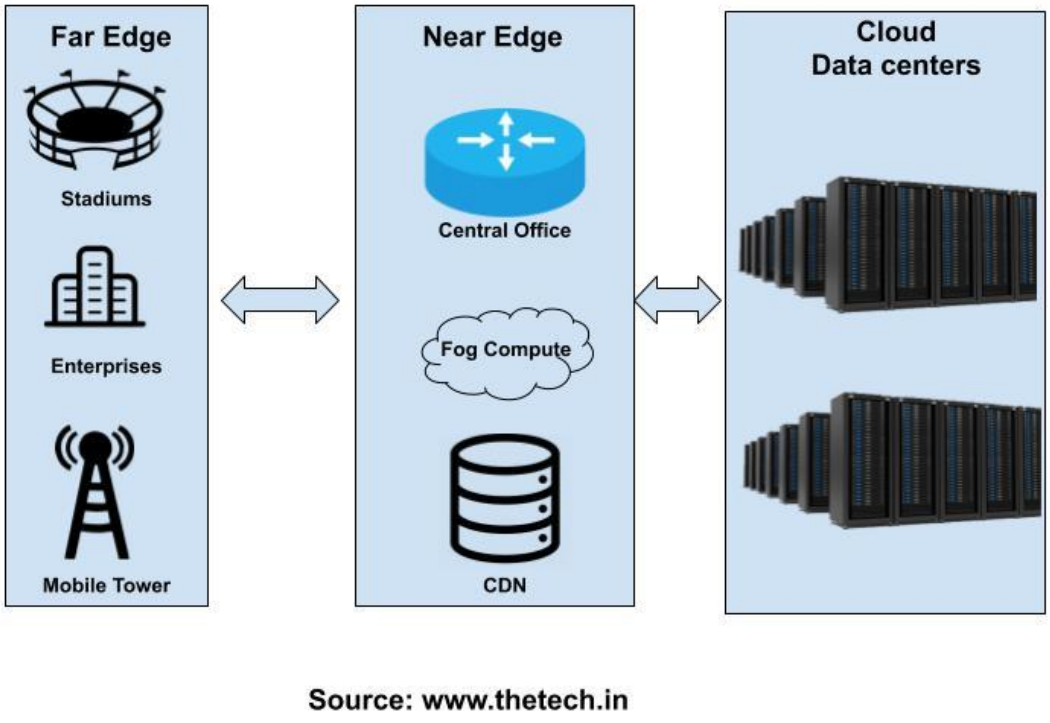

Figura 11 – *Near-edge deployment* (https://tinyurl.com/yfhcjad6)

5.5. Segurança

Duas visões com relação a segurança de rede foram expostas. A primeira que entende que a padronização e a existência de vários players são suficientes para garantir a segurança. A segunda entende que a existência de mais interfaces do que as atualmente padronizadas pelo 3GPP e a exposição dessas interfaces, especialmente em sites remotos, podem prejudicar a segurança.

5.6. Ações a serem propostas e em andamento pelo Governo Federal

Gestores do Funttel se comprometeram em avaliar a possibilidade de incluir desenvolvimento de equipamentos *OpenRAN* dentro das previsões de recurso do fundo.

Há estudos para se utilizar os recursos advindos da Lei da informática (aplicar 4% da receita em P&D) e colocar dentre os focos o desenvolvimento de equipamentos ou *software* de rede aberta.

Há também iniciativas que estão pensando para a capacitação de profissionais para o aperfeiçoamento e treinamento de recursos humanos.

6. ETAPA 2 – ANÁLISE

Após a etapa de mapeamento, vem à tona o momento de realizar análises sob diferentes perspectivas, de modo a evidenciar os diferentes pontos de vista e os diferentes contextos de pesquisa. Com a finalidade de permitir um maior detalhamento dos diferentes pontos de interesse, a segunda etapa foi dividida em quatro ramos paralelos, uma para cada subgrupo predefinido:

- Subgrupo 1A – Interoperabilidade
- Subgrupo 1B – Segurança
- Subgrupo 2 – Aspectos econômicos
- Subgrupo 3 – Aspectos regulatórios

Assim, foi possível desenvolver exame minucioso de cada aspecto que envolve a tecnologia de redes de acesso abertas.

6.1. Subgrupo 1A – Interoperabilidade

Prova de Conceito (PoC) do inglês *Proof of Concept* é simular em laboratório com fidelidade e baixo custo situações de uso do *design* da solução a ser desenvolvida para demonstrar a configuração compatível de vários fornecedores, desempenho e recursos de gerenciamento de falhas. O que permite identificar potenciais problemas de naturezas muito diversas, onde diferentes fornecedores e operadoras podem se reunir para atingir metas de interoperabilidade, além de detalhes práticos de implementação. Durante o PoC descobre-se com que grau de eficácia um novo produto ou serviço atende necessidades específicas do consumidor. Além da verificação para garantir a

interoperabilidade com RAN multi-fornecedor, as simulações devem ser capazes de testar o desempenho incluindo *throughput*, mobilidade e estabilidade sob os vários tipos de ambiente em uma rede comercial. Porém, como demonstrado na subseção Arquitetura e Interfaces, as situações reais podem ser mais desafiadoras do que simulações em ambiente de laboratório.

6.1.1. Teste de integração e interoperabilidade

A separação do equipamento da estação base em vários componentes (RU, DU e CU) com base no conceito de *OpenRAN* permite que os operadores selecionem produtos com flexibilidade. No entanto, essa flexibilidade requer que os operadores selecionem e integrem adequadamente os produtos. Também é necessário confirmar se as funções e o desempenho exigidos são alcançados de maneira adequada por meio de um processo de prova de conceito ou teste de verificação. Mesmo quando os fornecedores implementam uma interface aberta de acordo com a especificação definida pela organização padrão, como 3GPP e O-RAN *Alliance*, a interpretação das novas especificações pode, às vezes, ser diferente entre os fornecedores. Portanto, até que a especificação se torne estável, a verificação por meio de testes de interoperabilidade para conectar produtos de diferentes fornecedores é importante.

O processo de verificação consiste em estabelecer a base de testes, projetar o conteúdo da verificação e realizar testes com produtos de diferentes fornecedores. Porém, durante as reuniões levadas a cabo pelo GT, foi apontada pelos fornecedores a dificuldade de se montar *setup* completo para ensaios para certificação dos elementos da *OpenRAN*, que poderia impedir a entrada de novos *players*. Foi informado que nem todos os fabricantes produzem todos os módulos, como exemplo, foi citada a dificuldade de fornecedores de RU encontrarem fornecedores de DU e CU para realização de ensaios. Foi enfatizada também a característica intrínseca da *OpenRAN* de desagregação.

Entretanto, representantes dos laboratórios habilitados pela Anatel para ensaios de certificação de produtos cogitam o uso de simuladores e emuladores, mas ainda estão em fase de análise de viabilidade e citaram a regra disposta no ato Anatel nº 4083 de 31 de julho de 2020, item 6.3.1.3, que é "de responsabilidade do requerente o envio da amostra devidamente identificada e totalmente preparada para os ensaios".

De outro lado, as operadoras mencionaram que todos os testes demandaram *setup* completo, que foi possível através da figura de um integrador (responsável pelos testes), que providenciou toda a estrutura necessária.

Representantes de OCDs (Organismos de Certificação Designados) comentaram que é importante definir escopo e que conceitos macros não diferem das redes legadas. Conceitos funcionais, de segurança, espectro e meio ambiente já são testados. Outro ponto importante é que ensaios de certificação são diferentes de testes de conformidade das operadoras.

Quando questionado posicionamento da Anatel em relação à necessidade de teste de interoperabilidade ou somente de RF, foi mencionado que a Agência atua sua

competência na interface aérea e não nos procedimentos de teste de interoperabilidade. Frisa-se também que mesmo na interface aérea, não interfere na definição dos protocolos definidos por organismos internacionais, como exemplo 3GPP e O-RAN *Alliance*.

Embora tenha sido questionado aos participantes do GT sobre soluções que os *players* internacionais estão desenvolvendo em outros países, não houve resposta até a elaboração desse relatório.

6.1.2. Histórico de interoperabilidade no âmbito da Anatel

No início das comunicações móveis digitais, chamado de segunda geração (2G), a BTS (*Base Transceiver Station*, Estação Rádio Base) GSM (*Global System for Mobile Communications*, Sistema Global para Comunicações Móveis) não possuía inteligência, de tal sorte ser necessária a conexão dela com a BSC (*Base Station Controller*, Controladora da Estação Base) que a controlava, formando com ela a BSS (*Base Station Subsystem*, Subsistema da Estação Base). Por meio da interface Abis, que conectava a BTS à BSC, a segunda podia controlar os equipamentos e a alocação de recursos na primeira.

Em redes 2G, que continuam em operação, a BSC tem como função alocar um canal para a duração da chamada, monitorar as chamadas visando qualidade e potência transmitida pela BTS ou a estação móvel e garantir o *handover* para outra célula, quando requerido.

Para os ensaios de certificação da BTS, é possível o uso de emuladores que realizam a ativação do dispositivo ensaiado através da interface Abis, sem necessidade de acoplamento de uma BSC real. A interoperabilidade entre a BTS e a BSC e a entre a BTS e o emulador não são tópicos dos ensaios de certificação da Estação Rádio Base.

Fica, desta maneira, explicitado que a Agência não tem como histórico determinar verificação de protocolos de conexão em redes móveis em ensaios de certificação. Mais do que isso, a interoperabilidade entre módulos da rede, assim como da rede com os equipamentos que a usam, é requisito prévio para o atendimento satisfatório dos usuários das prestadoras de serviço de comunicações móveis. Logo, a princípio, entende-se que não será necessário ajustes aos processos de certificação de BTS para o acolhimento da tecnologia *OpenRAN* pelo mercado brasileiro de telecomunicações.

6.1.3. Especificações

Há pouco mais de três anos, a possibilidade de misturar e combinar componentes de rede de diferentes empresas, a chamada *OpenRAN*, passou de um simples conceito para várias implantações importantes em todo o mundo com o objetivo de fomentar a concorrência e reduzir os custos. Há duas vertentes na indústria sobre como as redes sem fio devem ser construídas. A primeira, composta pelos apoiadores do uso de redes aberta que sustentam que, com a abertura, surgirão imensas inovações e haverá redução dos custos do acesso sem fio. Porém, a segunda vertente acredita que, se

implementada, danificaria ou até destruiria o modelo de negócio existente, comprometendo inclusive a segurança básica da rede.

Assim, o momento é de escolha na indústria de comunicações, seja pela adesão e definição dos termos para o desenvolvimento e implementação da *OpenRAN* ou pela continuidade do fornecimento dos equipamentos de telecomunicações da forma atual, que as operadoras de rede vêm utilizando por anos.

A rede de acesso de rádio como uma estação base de celular ou torre é a estrutura que conecta um dispositivo final, como um telefone celular, à rede principal com fio. Primeiramente as antenas da torre de celular recebem o sinal do telefone. Em segundo lugar, um rádio converte o sinal analógico em digital. Terceiro, um componente chamado unidade de banda base processa o sinal, corrige erros e, finalmente, o transmite para a rede central. Dentro da RAN, esses componentes, a antena, o rádio e a unidade de banda base, são denominados como blocos distintos de tecnologia. Mesmo que cada unidade de banda base seja desenvolvida e construída de forma independente, suas interfaces devem ser compatíveis. Caso contrário, os dados podem ser distorcidos ou perdidos ao passar do rádio para a unidade de banda base ou vice-versa. Todavia, atualmente não há garantia de que um rádio fabricado por um determinado fornecedor será interoperável com uma unidade de banda base fabricada por outro fornecedor.

As especificações para os padrões de interface RAN, como as especificações para redes celulares, incluindo interfaces de cobertura, são definidos pelo 3GPP e são projetadas considerando a interoperabilidade, onde vários fornecedores poderiam participar do ecossistema com propósito de evitar a dependência excessiva de operadoras em um único fornecedor. Não obstante, com o avanço da tecnologia, surgiu a possiblidade de solução RAN desagregada, onde a banda base pode ser dividida em vários componentes e esses componentes podem interagir com os de outros fornecedores de RAN. Porém, não há nada que impeça um fornecedor de "complementar" uma interface padronizada com técnicas proprietárias adicionais[23]. A O-RAN *Alliance*, formada em 2018, tem entre seus objetivos unificar e impulsionar essa desagregação e abertura, a fim de promover mais competição e consequentemente reduzir custo.

De acordo com a Associação GSM, as operadoras gastam grande parte do orçamento em infraestrutura, equipamentos e tecnologias 5G para suas redes. A RAN consome a maior parte dessas despesas de capital. A Associação GSM prevê que em 2025 as operadoras gastarão até 86% de seus orçamentos de capital em RAN[24]. Diante disso, as operadoras buscam alternativas para evitar qualquer problema causado por *hardware* incompatível. E uma maneira segura de evitar tal incompatibilidade é optar pelo mesmo fornecedor de uma ponta da rede para a outra, evitando assim qualquer

[23] *Small Cell Forum*. 2021. Disponível em: <https://www.smallcellforum.org/>. Acesso em: 22.09.2021.
[24] The Cellular Industry's Clash Over the Movement to Remake Networks. 2021. Disponível em: <https://spectrum.ieee.org/ the-cellular-industrys-clash-over-the-movement-to-remake-networks>. Acesso em: 22.09.2021.

possibilidade de interfaces incompatíveis. Porém, o fator inquietante por parte das operadoras é o número reduzido de empresas que podem fornecer serviços de redes ponta a ponta.

Uma versão mais arrojada propõe dividir a *OpenRAN* em componentes menores além do rádio e a unidade de banda base, conforme seção Arquitetura e Interfaces. Esta desagregação é uma característica das especificações 5G. A vantagem de dividir a unidade de banda base em CU e DU é que a CU não precisa mais estar localizada na própria torre de celular. Em vez disso, uma única CU pode ficar em um *farm* de servidores local, mantendo a conexão com a rede central para várias torres de celular na área.

A O-RAN *Alliance* propõe também outras divisões para criar mais oportunidades para desagregação além da divisão entre a unidade distribuída e a unidade centralizada. O objetivo da criação dessas divisões, chamadas de *splits*, é permitir que as operadoras adquiram componentes mais adaptados para o tipo específico de rede que estão construindo. Para isso, uma divisão importante, chamada *split* 7.2x (seção *Splits* mais recomendadas), possui funções práticas como codificação e decodificação de sinal, bem como modulação, na unidade distribuída. Do outro lado da divisão, o rádio executa algumas tarefas de processamento leve, como formação de feixes, que estabelece a direção específica de uma transmissão. O rádio também é responsável por converter sinais digitais para sinais analógicos e vice-versa.

Outra divisão, a *split* 8, transfere até mesmo a responsabilidade pela formação do feixe para a unidade distribuída, deixando o rádio responsável apenas pela conversão dos sinais. Em contraste, a *split* 2 transfere codificação, decodificação, modulação, formação de feixe e ainda mais responsabilidades de processamento para o rádio, deixando a unidade distribuída responsável apenas por compactar os dados em menos bits antes de transferir os dados para a unidade centralizada. Dessa forma, como exemplo, um operador pode optar pela *split* 8 para uma implantação em grande escala exigindo muitos rádios. Com esta divisão é permitido o uso de rádios mais simples e, portanto, mais acessíveis, uma vez que todo o processamento acontece na unidade centralizada.

6.1.4. Plataforma RIC

É tecnicamente possível montar uma RAN desagregada com interfaces abertas usando apenas *hardware*, mas definir os componentes no *software* tem algumas vantagens. Para não centralizar todas as funções no *hardware*, a O-RAN *Alliance* também está incentivando a indústria sem fio a incorporar mais *software* à RAN. Atualizar um componente virtual pode ser mais simples.

A ênfase no *software* também está possibilitando que a indústria considere tecnologias totalmente novas, a mais importante delas é o RAN *Intelligent Controller*, RIC. O RIC coleta dados dos componentes RAN de dezenas ou centenas de estações base de uma vez e usa técnicas *machine-learning* para reconfigurar as operações de rede em tempo real. Ele baseia as modificações no fato de que as torres de celular trabalham sob uma carga de tráfego pesado, por exemplo, ou transmitindo em uma forte tempestade

de chuva que pode desvanecer os sinais. O RIC pode reprogramar os componentes de software da RAN para oferecer um serviço melhor.

A O-RAN *Alliance* especificou[25] a estrutura RIC e as interfaces correspondentes considerando dois módulos diferentes, mostrados na Figura 2 – Interfaces da arquitetura *OpenRAN* (https://tinyurl.com/yjy4ao4e), *near real time* RIC e *non real time* RIC, para atender a requisitos de serviço de rede ainda maiores de diferentes operações com automação. A separação da funcionalidade RIC de acordo com diferentes escalas de tempo, *non* RT e *near* RT, visa facilitar a redução nos custos de desenvolvimento e implantação e ajudar a padronizar e expandir o ecossistema em tempo hábil. Além disso, projetar funcionalidade RIC *non* RT em uma plataforma de gerenciamento e orquestração de serviços (SMO), mas não na RAN em si, visa proteção de acesso a informações contextuais e otimização coordenada de recursos de rádio e políticas de rede.

Pode-se listar casos de uso de aplicativos promissores para RIC como o gerenciamento proativo de recursos de rádio, a otimização de *massive* MIMO e a mitigação de interferência. Também podem ser citados outros aplicativos sistemáticos, como de divisão de rede ponta a ponta, monitoramento de KPIs e detecção de anomalias. Mas a lista não se limita aos casos reais de uso do aplicativo RIC, dependendo do ambiente de implementação específico no mercado consumidor ou no mercado corporativo, mais casos de uso podem ser introduzidos para garantir o nível de serviço, como exemplo, de estimativa de canal altamente preciso e de economia de energia.

O RIC *near* RT é responsável por criar uma plataforma de *software* para um conjunto de xApps para a RAN; O RIC *non* RT fornece funcionalidade de configuração, gerenciamento e análise. Ao desagregar o *software* do *hardware* e desenvolver interfaces padronizadas e *designs* de referência abertos, uma arquitetura de rede flexível e ágil deve ajudar na economia de TCO e oferecer aos usuários finais Qualidade de Experiência (*Quality of Experience*, QoE) otimizada. Assim, o RIC e o desenvolvimento de xAPPs e rAPPs correspondentes tem atraído muita atenção no mercado de telecomunicações.

Os aplicativos representam uma extensão de um RIC[26], seja um rAPP para o RIC *non* RT ou um xAPP para o RIC *near* RT. Os aplicativos nesses dois ambientes diferentes têm mecanismos de plataforma diferentes, no entanto, eles compartilham um comportamento comum, permitindo que uma camada de abstração forneça a capacidade do aplicativo a ser desenvolvido de forma que possa ser implantado em qualquer ambiente a partir do mesmo pacote. O RIC *near* RT interage com o RIC *non* RT por meio da interface A1 para receber os modelos treinados e executá-los para melhorar as condições da rede. O RIC *near* RT pode ser implantado em um modelo

[25] ABI, R. M. R. Ric will upset telco applecarts as it becomes the os for future 5g ran. 2021. Disponível em: <https://www.telecomtv.com/content/open-ran/ric-will-upset-telco-applecarts-as-it-becomes-the-os-for-future-5g-ran-41594/>. Acesso em: 06.10.2021.
[26] KINSEY, D. Application deployment use case. 2021. Disponível em: <https://wiki.o-ran-sc.org/display/RSAC/2.+Application+Deployment+Use+Case>. Acesso em: 06.10.2021.

centralizado, como mostrado na Figura 12 - Instalação centralizada do *near* RT RIC ou distribuído na Figura 13 - Instalação distribuída do *near* RT RIC, dependendo da topologia da rede.

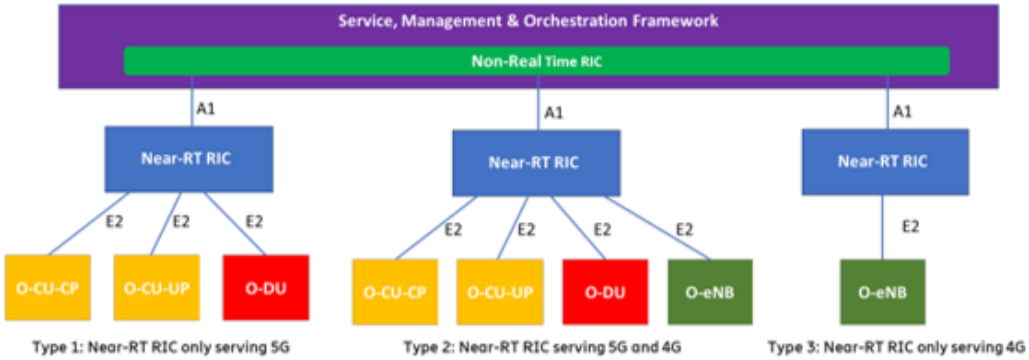

Figura 12 - Instalação centralizada do *near* RT RIC

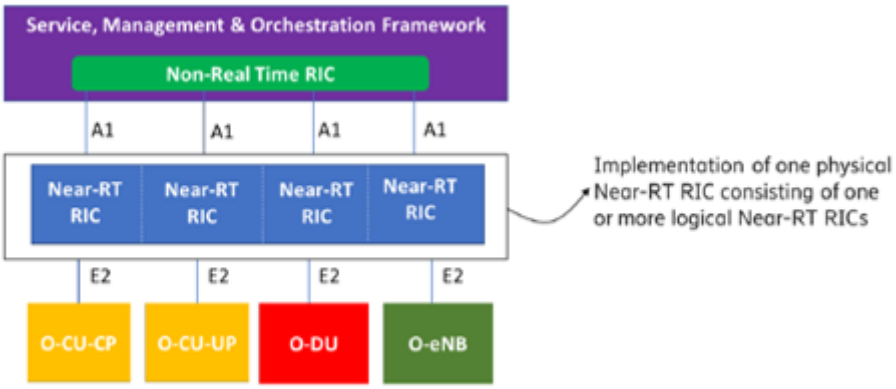

Figura 13 - Instalação distribuída do *near* RT RIC

6.1.5. Interoperabilidade – Conclusão e aspecto futuro

Esta seção apresentou considerações em relação à interoperabilidade da topologia *OpenRAN* no que se refere ao *setup* de testes, às especificações e ao RIC. Verificou-se que o RIC ajuda a desacoplar os planos de controle e dados da RAN o que contribui para a elaboração de uma rede de rádio inteligente e em constante evolução, promovendo um ecossistema de aplicativos de *software* que podem controlar vários aspectos da RAN, alimentados pelos avanços mais recentes em ML e IA, conforme descrito pela sua arquitetura funcional e de *software*.

Como trabalhos futuros para o GT *OpenRAN*, subgrupo interoperabilidade, podem ser citados o acompanhamento das entregas dos diferentes *stakeholders* pertencentes ao ecossistema *OpenRAN*, a análise e divulgação dos resultados dos estudos e pesquisas realizados pela parceria que a Anatel firmou com a Universidade de Brasília – UnB e investigação da virtualização de rede e seu papel na interoperabilidade de redes abertas.

6.2. Subgrupo 1B – Segurança

O 5G *New Radio* (5GNR) foi a primeira etapa implantada pelas operadoras móveis em arquiteturas 5G *Non Stand Alone* (NSA), uma vez que a rede de acesso de rádio 5G (*Radio Access Network*, RAN) é um componente fundamental para habilitar os recursos básicos do 5G: grande largura de banda (eMBB), escala maciça (mMTC) e alta confiabilidade e baixa latência (URLLC)[27].

> Banda larga móvel aprimorada (*enhanced mobile broadband*, eMBB): refere-se às taxas de transmissão de dados média e de pico desejadas, capacidade e cobertura superiores em comparação à banda larga móvel convencional. O eMBB especifica um *design* 5G capaz de suportar até 20 gigabits por segundo (Gbps) no *downlink* (DL) e 10 Gbps no *uplink* (UL).
>
> Comunicações maciças do tipo máquina (*massive machine-type communications*, mMTC): suportam acesso 5G IoT por bilhões de dispositivos e sensores conectados. Os casos de uso previstos cobrem desde dispositivos de baixa taxa de dados e largura de banda com rajadas infrequentes de dados que exigem bateria de longa duração bem como dispositivos de largura de banda e taxa de dados muito alta.
>
> Comunicações ultraconfiáveis e de baixa latência (*ultra-reliable and low-latency communications*, URLLC): concentram-se em aplicativos que exigem comunicações em tempo real e à prova de falhas. Os exemplos incluem veículos autônomos, internet industrial, redes inteligentes, proteção de infraestrutura e sistemas de transporte inteligentes.

Hoje, as redes públicas 5G estão oferecendo banda larga móvel aprimorada para um número crescente de consumidores e empresas, ao mesmo tempo em que atendem a um número crescente de dispositivos conectados. Este impacto é visto no Brasil, que recentemente realizou o leilão de frequências para utilização por redes 5G[28]. Conforme a computação de ponta evolui, o 5G *Stand Alone* (SA) é implantado e os padrões continuam a evoluir, o 5G pode atingir as metas estipuladas de capacidade, latência, desempenho. Também oriundo do leilão 5G, o Brasil será o primeiro país da América Latina a utilizar o 5G SA[29]. Não obstante, o Ministério da Ciência, Tecnologia e Inovações assinou acordo de cooperação com recursos para desenvolvimento da arquitetura aberta no Brasil[30].

Para atender à hiperescalabilidade, alto desempenho e baixa latência exigidos por casos de uso 5G futuros, o 5G NR é distribuído, virtualizado, compartilhado e é arquitetonicamente mais complexo do que as gerações anteriores. Benefícios claros são

[27] https://www.fortinet.com/blog/industry-trends/the-growing-need-for-4g-and-5g-radio-access-network-ran-security
[28] https://www.gov.br/pt-br/noticias/transito-e-transportes/2021/11/leilao-do-5g-confirma-expectativas-e-arrecada-r-47-2-bilhoes
[29] https://www.gov.br/mcom/pt-br/noticias/2021/novembro/brasil-e-o-primeiro-pais-da-america-latina-a-adotar-o-5g-standalone
[30] MCTI assina acordo de cooperação com recursos para programa de Open RAN | TELETIME News

trazidos por esses recursos, mas novos riscos e desafios de segurança são introduzidos e ampliados. Esses riscos e desafios devem ser tratados por meio de controles de segurança apropriados projetados para apoiar e proteger a entrega de serviços 5G NR em quaisquer nuvens das operadoras.

Especificamente com relação a redes abertas, vulnerabilidades que residem em pilhas de *software* desatualizadas junto com problemas possíveis na interface aérea agora estão encontrando a nova geração de ameaças de rádio com novas interfaces, aplicativos crescentes, virtualização e conteinerização que, além disso, aumentaram drasticamente a superfície de controle para equipe de segurança cibernética das operadoras. Tais características podem permitir a implementação de uma ampla variedade de ataques, como interceptação de dados, acesso a informações confidenciais, violação de operação de rede e outros[31].

A arquitetura *OpenRAN* difere da arquitetura RAN tradicional, que é baseada nos moldes do Projeto de Parceria de 3ª Geração (3rd *Generation Partnership Project*, 3GPP). De um lado a abordagem aberta garante uma solução mais flexível e econômica com *software* de terceiros, mas, do outro, há novos componentes, interfaces, pilhas de *software* e tecnologias para serem protegidos. Novos *stakeholders* surgiram e novos modelos de negócios podem ser aplicáveis. A superfície de ataque pode estar se tornando maior: o *design* e a implantação da arquitetura *OpenRAN* poderão gerar vários desafios de segurança por causa das novas interfaces e componentes específicos, as técnicas de virtualização e conteinerização, o suporte de código-fonte aberto, a capacidade de suportar um modelo de inteligência artificial (AI) ou *machine learning* (ML), etc. Devido a estas razões, a análise de segurança e o modelo de ameaça para *OpenRAN* devem ser cuidadosamente estudados e vulnerabilidades, ativos, ameaças, requisitos, contramedidas e recomendações relevantes devem ser identificados para reduzir riscos.

Salienta-se que o Escritório Federal de Segurança da Informação da Alemanha (*Bundesamt für Sicherheit in der Informationstechnik*, BSI) elaborou relatório de análise de riscos[32] sobre a arquitetura *OpenRAN*. Como resultado verificou-se que há muitas interfaces e componentes especificados de médio a alto risco de segurança, pois o atual processo de desenvolvimento de especificações *OpenRAN* não segue o paradigma orientado ao tripé "segurança / privacidade por *design* / padronização", de acordo com o escritório, como também os princípios de *Zero Trust* (ou segurança multilateral, trata-se de confiabilidade mínima em relação a todas as partes envolvidas) não foram levados em consideração. Para superar tais adversidades, o BSI sugere em seu relatório a adoção dos seguintes procedimentos:

- Introdução obrigatória de medidas de segurança opcionais estabelecidas pela O-RAN *Alliance*.

[31] https://www.linkedin.com/pulse/rano-ran-security-new-opportunities-beside-old-mnos-paolo-emiliani/?trk=articles_directory

[32] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/5G/5GRAN-Risikoanalyse.html?nn=520690

- *Backup* ponta-a-ponta dos dados do plano do usuário entre equipamento do usuário (*user equipment*, UE) e core 5G.
- Maior consideração do paradigma "segurança / privacidade por *design* / padronização".
- Consideração dos princípios de *Zero Trust*.

Este relatório possui foco na aplicação da abordagem *Zero Trust* em redes abertas.

6.2.1. Segurança de Redes

Com o 5G, as redes se tornam cada vez mais distribuídas e mais componentes são movidos para a borda da rede, criando a necessidade de melhor segurança. A IoT maciça aumenta o número de dispositivos na borda da rede exponencialmente. Em 2026 estima-se que haverá 5,4 bilhões de conexões IoT celulares[33] – mais de três vezes a quantidade de conexões IoT celulares em 2020. Os requisitos de segurança para infraestrutura de rede, dispositivos e consumidores aumentam enormemente com 5G. O 5G também precisa preencher as lacunas de segurança das gerações anteriores de tecnologia celular na autenticação do usuário e criptografia de dados. 5G traz dois aprimoramentos de segurança importantes:

- Autenticação de assinante baseada em localização para permitir que apenas assinantes reais acessem serviços de rede.
- Adaptação de nível de segurança com divisão de rede para aumentar o nível de segurança para redes virtuais ou serviços específicos.

Aproveitando a criptografia, o 5G oferecerá um nível mais alto de segurança entre as redes de diferentes operadoras móveis e controlará o acesso aos serviços de rede. A criptografia mais forte (algoritmos de 256 bits versus 128 bits em 4G) também ajudará as redes 5G a abordarem possíveis ataques de computadores quânticos.

O 3GPP recomenda o uso de *Security Gateways* (SecGWs) para proteger as comunicações RAN e RAN para Núcleo para garantir a continuidade do serviço e confidencialidade. O 3GPP *Security Gateway* conta com IPSec[34] e recursos de gerenciamento de certificados para fornecer controle de acesso por meio de autenticação e confidencialidade e integridade de tráfego por meio de criptografia. A autenticação e a criptografia podem ser estendidas ao plano do usuário (*user plane*, UP), ao plano de controle (*control plane*, CP), bem como ao tráfego de operação e gerenciamento.

Neste contexto, é possível inferir que AI e ML exercerão papel fundamental nas redes 5G, tanto na sua operação quanto na garantia de sua segurança. A grande largura de

[33] https://www.ericsson.com/en/reports-and-papers/mobility-report/reports/june-2021
[34] Protocolo de Segurança IP é uma extensão do protocolo IP que visa a ser o método padrão para o fornecimento de privacidade do usuário, integridade dos dados e autenticidade das informações ou prevenção de *identity spoofing*, quando se transferem informações através de redes IP pela internet.

banda, a baixa latência e a conectividade maciça de sistemas 5G requerem muita automação de segurança, impossível de ser alcançado sem AI e ML, que podem apoiar e automatizar operações de segurança e a análise de incidentes, encontrar e prever violações de segurança e adaptar-se dinamicamente às mudanças nas condições da rede.

Entretanto, AI e ML e seus papéis em segurança de redes possuem desafios. Apesar de trazerem soluções de segurança mais poderosas, também permitem oportunidades para novos tipos de ataques exclusivos de sistemas automatizados, que incluem técnicas como ataques de evasão de modelo (pequenas mudanças nos dados de entrada), ataques de extração de modelos (aprendizado ou roubo de modelos) e ataques de inversão de modelo (influências na construção do modelo). Como AI e ML dependem muito dos dados durante o desenvolvimento e a implantação, a segurança e a privacidade dos dados são uma preocupação relevante.

Outro aspecto importante que exerce influência em redes de acesso é a ampliação de seu uso. Para permitir a escalabilidade crescente fornecida por redes 4G e, especialmente, 5G, necessita-se implantar cada vez mais células menores. Muitas dessas femtocélulas, picocélulas e microcélulas 4G (estações eNobeB ou eNB) e 5G (estações gNodeB ou gNB) estarão localizadas em áreas públicas e em outros locais não seguros. Haverá casos também onde elas serão conectadas à rede da operadora por meio de um backhaul não confiável. Esses fatores representam um risco crescente, contribuindo para um aumento na superfície de ataque, bem como o risco de adulteração, uso indevido e manipulação do tráfego.

Outro ponto de atenção, o RAN *sharing* 5G é um método cada vez mais popular usado por operadoras 5G para aumentar sua cobertura de maneira econômica. Envolve o compartilhamento de RAN 5G entre duas ou mais operadoras móveis, oferecendo mutuamente acesso aos recursos uma do outra para melhor servir os clientes e reduzir os custos associados às implantações de redes 5G NR. Isso é especificamente interessante em frequências 5G mais altas, especialmente nas faixas de frequências milimétricas (*millimiter wave*, mmWave) com um alcance mais limitado, onde os custos de implantar mais estações rádio base são significativos. Para garantir a separação, privacidade e segurança do UP e do CP entre os operadores de compartilhamento, ferramentas de segurança apropriadas devem ser implantadas.

A evolução contínua do 4G e a introdução do 5G estão permitindo a implementação de casos de uso verticais e de negócios que fornecem valor além da simples conectividade sem fio. No entanto, eles também colocam uma importância crescente na integridade e continuidade do tráfego do UP na RAN, bem como no core de rede. O UP agora é um dos principais componentes da rede das operadoras capaz de fornecer serviços de maior valor agregado (*value-added services*, VAS), como *infotainment*, serviços de IoT, de realidade aumentada (*augmented reality*, AR) e de realidade virtual (*virtual reality*, VR), como exemplo. Isso, por sua vez, leva à necessidade de maior segurança, integridade e continuidade dos dados do UP, que provavelmente também experimentarão um crescimento significativo.

A necessidade de melhor desempenho da RAN, agilidade, escalabilidade, flexibilidade e custo-benefício levou à sua evolução gradual das redes 4G LTE e, finalmente, das 5G NR. Como resultado, as operadoras operarão um ambiente RAN híbrido composto de diferentes arquiteturas de eNB e gNB centralizadas, distribuídas, virtualizadas e em nuvem. Essas arquiteturas também dependerão dos requisitos específicos de caso de uso por segmento de mercado ou *slice* de rede. Em tal ambiente híbrido, manter a segurança, integridade e visibilidade para CPs, UPs e organização e manutenção (*organization and management*, O&M) requer o uso de um conjunto comum de ferramentas de segurança flexível o suficiente para se adaptar às diferentes arquiteturas, requisitos e restrições da RAN.

4G LTE-A e, principalmente, 5G NR fornecem a capacidade de oferecer suporte a casos de uso críticos e inovação em diferentes setores, incluindo saúde, energia e transporte. Ao contrário das gerações móveis anteriores, a padronização da tecnologia de infraestrutura móvel e a crescente dependência de seus serviços para alguns casos de uso críticos aumentarão o interesse em ataques cibernéticos à infraestrutura móvel, impulsionando ainda mais a necessidade crescente de segurança de RAN.

Não obstante, para combater efetivamente as sofisticadas ameaças cibernéticas de hoje contra ambientes de TI modernos com suas defesas focadas em seus perímetros, um novo paradigma para o gerenciamento de acesso privilegiado pode ser necessário para estabelecer a identidade como o novo perímetro, *Zero Trust Privilege*, ou privilégio de confiança zero, baseado na tríade "nunca confie, sempre verifique, aplique o menor privilégio", seja o acesso solicitado de dentro ou de fora da rede. *Zero Trust Privilege* requer a concessão de acesso de privilégio mínimo com base na verificação de quem está solicitando acesso, o contexto da solicitação e o risco do ambiente de acesso. Ao implementar o acesso com privilégios mínimos, as organizações diminuem sua superfície de ataque e facilitam auditorias e conformidade, além de reduzirem o risco, a complexidade e os custos[35].

6.2.2. *Zero Trust Architecture*

Zero trust (ZT), também chamado segurança multilateral, é o termo para um conjunto em evolução de paradigmas de segurança cibernética que transferem o foco das defesas de perímetros estáticos baseados em rede para abranger usuários, ativos e recursos. Interessante notar que o foco deixa de ser os dados, como em uma abordagem tradicional, e passa a ser os recursos, que incluem dados, sistemas e aplicações. Uma arquitetura de confiança zero[36] (*Zero Trust Architecture*, ZTA) usa princípios de confiança zero para planejar a infraestrutura e os fluxos de trabalho industriais e empresariais. A confiança zero assume que não há confiança implícita concedida a ativos ou contas de usuário com base exclusivamente em sua localização física ou de rede, seja redes locais ou internet, ou com base na propriedade de ativos, como empresa ou propriedade pessoal. Autenticação e autorização de assunto e dispositivo são funções discretas executadas antes que uma sessão para um recurso corporativo

[35] Miller, L. George, T. *Zero Trust Privilege For Dummies*. Hoboken, NJ, John Wiley & Sons, Inc. 2019.
[36] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

seja estabelecida. A confiança zero é uma resposta às tendências de rede corporativa que incluem usuários remotos, *bring your own device* (traga seu próprio dispositivo, BYOD[37]) e ativos baseados em nuvem que não estão localizados dentro dos limites de uma rede corporativa. A confiança zero se concentra na proteção de recursos (ativos, serviços, fluxos de trabalho, contas de rede, etc), não em segmentos de rede, já que a localização da rede não é mais vista como o principal componente da postura de segurança do recurso.

A ZTA é uma abordagem ponta-a-ponta para recursos corporativos e segurança de dados que abrange identidade de entidades pessoais e não pessoais, credenciais, gerenciamento de acesso, operações, terminais, ambientes de hospedagem e a infraestrutura de interconexão. O foco inicial é restringir os recursos para aqueles que precisam acessar e conceder apenas os privilégios mínimos, como ler, gravar e excluir, necessários para realizar a missão. ZTA difere de uma abordagem tradicional de segurança, onde os sujeitos recebem acesso autorizado a uma ampla coleção de recursos uma vez que estejam na rede interna. Como resultado, o movimento lateral não autorizado dentro do meio ambiente tem sido um dos maiores desafios para garantir a segurança em tais redes. Estas abordagens tradicionais, baseadas em conexões confiáveis de Internet (*trusted internet connections*, TIC) e em *firewalls* de perímetro, não possuem recursos para proteção conta ataques internos e para garantia de ações lícitas fora dos perímetros de segurança, como trabalho remoto, serviços em nuvem e *edge devices*.

Para diminuir as incertezas, o foco da ZTA está na autenticação, autorização e redução de zonas de confiança implícitas, enquanto mantém a disponibilidade e acelera mecanismos de autenticação. As regras de acesso são feitas de forma mais granular possível para impor o mínimo de privilégios necessários para executar a ação na solicitação. Em uma rede ZTA, não se permite tráfego desconhecido. O tráfego desconhecido mostra que o modelo de confiança foi quebrado e precisa ser corrigido.

Uma rede ZTA também necessita de um processo contínuo de acompanhamento da segurança, ou seja, examinar continuamente todos os *logs* internos e externos por meio da camada 7 do modelo OSI (*open systems interconnect*, interconexão de sistemas abertos) e focar nos aspectos operacionais segurança, sendo essencial inspecionar e registrar todo o tráfego na rede[38]. Uma rede *Zero Trust* possui três propriedades[39]:

- Acesso de maneira segura de todos os recursos, independentemente de sua localização física ou lógica.
- Política de controle de acesso rígida.
- Captura e *log* de todo tráfego.

[37] Conceito de infraestrutura oriundo do mercado de TI, trata-se da utilização de aparelhos dos próprios funcionários para desempenhar as atividades empresariais.
[38] https://www.paloaltonetworks.com/cyberpedia/zero-trust-5-step-methodology
[39] https://ieeexplore.ieee.org/document/9418203

Baseados nestas três propriedades, o planejamento e a implementação de uma rede, para garantir acesso *Zero Trust*, deve assumir que:

- A rede local não é uma zona de confiança implícita.
- Dispositivos conectados, especialmente devido à tendência BYOD, não são uma entidade da empresa, pois qualquer dispositivo pode ser comprometido.
- Recursos nunca são confiáveis, ou seja, do ponto de vista da segurança, todos os ativos ou recursos devem ser avaliados continuamente e só podem estar em uso enquanto for necessário.
- Nem todos os recursos de uma organização estão em sua infraestrutura, o que é explicitado por serviços em nuvem, que se tornaram uma parte essencial de toda rede corporativa.
- Todas as solicitações de conexão fora da empresa, como a área de trabalho remota, devem ser autorizadas e autenticadas. Todos os dados devem ser comunicados com respeito, confidencialidade, integridade e autenticação de origem.
- Com base nas premissas mencionadas acima, o ponto crucial é que todos os ativos e comunicações de dados entre a infraestrutura corporativa e não corporativa devem estar continuamente sob a estratégia e postura de segurança.

Assim, para a implantação de uma rede *Zero Trust*, pode-se seguir os seguintes passos[40]:

- Identificar a superfície de proteção.
- Mapear os fluxos de transação.
- Construir uma arquitetura *Zero Trust*.
- Criar política de *Zero Trust*.
- Monitorar e manter.

6.2.3. ZTA em redes de acesso

Partindo do princípio de que uma rede já está invadida, garantir que um usuário só tenha acesso ao mínimo necessário para executar suas funções pode ajudar a impedir ataques internos. Outras abordagens ZTA podem fortalecer as defesas de rede, como autenticação contínua e permissão de acesso apenas durante o uso.

Em redes de acesso, há padrões 3GPP 5G que suportam uma abordagem *Zero Trust* em três domínios[41], segurança de acesso à rede, segurança de domínio de rede e

[40] https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture

segurança de domínio de arquitetura baseada em serviço (*service-based architecture*, SBA).

A segurança de acesso à rede fornece aos usuários acesso seguro aos serviços por meio do dispositivo (telefone celular ou dispositivo IoT conectado) e protege contra ataques na interface aérea entre o dispositivo e o rádio. A segurança de domínio de rede inclui recursos que permitem que haja troca de dados de sinalização e do usuário com segurança entre o rádio e as funções de rede (*network functions*, NFs). Já o 5G SBA é construído em tecnologia e protocolos web para permitir tecnologias de virtualização e contêiner e plataformas de processamento em nuvem. A segurança de domínio SBA especifica o mecanismo para comunicação segura entre NFs.

Diversas ações podem ser tomadas para incrementar a segurança de uma rede de acesso, tais como[42]:

- Menor privilégio por meio de microssegmentação para proteger as funções da rede 5G mais detalhadamente.
- Direcionamento de políticas de segurança sobre o acesso a dados e aplicativos.
- Proteção de cargas de trabalho da função de rede nativa da nuvem (*Cloud-Native Network Function*, CNF) em todo o ciclo de vida de CI/CD (práticas combinadas de integração contínua e entrega contínua).
- Monitoramento de todas as interações entre as funções de rede em todas as camadas.
- Melhor identificação de anomalias, inibindo ataques de negação de serviço distribuída (DDoS) por meio de automação e AI.
- Foco em segurança com solicitações de acesso, menos em perímetro.

6.2.4. ZTA em *OpenRAN*

Neste novo paradigma, uma corporação deve assumir confiança zero implícita e analisar e avaliar continuamente os riscos para seus ativos e funções de negócios e, em seguida, decretar proteções para mitigar esses riscos[43]. Em uma arquitetura *Zero Trust*, essas proteções geralmente envolvem a diminuição de acesso a recursos, como dados e recursos de computação, aplicativos e serviços, apenas para os assuntos e ativos identificados expressamente para tanto, bem como autenticar e autorizar continuamente a identidade e postura de segurança de cada solicitação de acesso. O suporte de uma arquitetura *Zero Trust* requer que cada componente *OpenRAN* esteja

[41] https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/zero-trust-and-5g
[42] https://www.paloaltonetworks.com/blog/2021/09/zero-trust-for-5g-digital-transformation/
[43] https://www.mavenir.com/blog/openran-security-based-on-zero-trust-architecture/

em conformidade com as funcionalidades e proteções estabelecidas. O-RAN *Alliance* identificou vários princípios orientadores para os estudos sobre segurança de rede:

- Suporte à integração com identidade externa, credencial e sistema de gerenciamento de acesso (*identity, credential, and access management*, ICAM) usando protocolos padrão da indústria.
- Requerimento de autenticação e autorização em todos os acessos.
- Suporte a controle de acesso baseado em função (*role-based access control*, RBAC).
- Implementação de confidencialidade e da verificação de integridade nas conexões entre *OpenRAN* e componentes externos.
- Suporte à criptografia de dados em repouso.
- Suporte à prevenção de *replay*[44].
- Implementação de geração e coleta de *log* de segurança para um gerenciamento externo de informações e eventos de segurança (*security information and event management*, SIEM).

Estes princípios, ao serem implementados em uma rede aberta, permitiria garantir segurança na comunicação de todas as interfaces. Cada interface deve possuir seu mecanismo de defesa, uns especificados pelo 3GPP, outros pela O-RAN *Alliance*. Independente de qual interface, a comunicação entre os diferentes módulos *OpenRAN* precisa ser protegida por criptografia, garantia de integridade e proteção contra *replay*.

Não obstante, a autenticação mútua deve ser usada para autenticar duas entidades entre si e configurar uma conexão criptografada segura entre elas. A autenticação mútua evitaria a introdução de NFs ou xAPPs (microsserviços extensíveis de terceiros contidos no *Near Real Time* RIC) não autorizados.

Por fim, recomenda-se que o uso de autoridades de certificação (CA) auditadas de acordo com um programa *WebTrust* a fim de promover a confiança nos servidores CA usados na arquitetura *OpenRAN* para autenticação de elementos de rede.

Alegações do mercado de telecomunicações indicam que a segurança em uma rede aberta é oriunda de: visibilidade dada a abertura do *fronthaul*, já que interfaces abertas e padronizadas removem vulnerabilidades ou riscos que vêm com a implementação proprietária e potencialmente não confiável; desagregação da arquitetura de rede, pois operadoras podem construir plataformas nativas em nuvem por meio de seleção de fornecedores confiáveis; desagregação da plataforma, que proporciona visibilidade e monitoramento automático da rede; adoção de melhores práticas da indústria no desenvolvimento de aplicativos em contêineres, como *DevSecOps* (abreviação de desenvolvimento, segurança e operações) "*secure by design*"; e teste automatizado no

[44] Um ataque de repetição, ou *replay attack*, é uma forma de ataque à rede em que a transmissão de dados válidos é maliciosa ou fraudulentamente repetida ou atrasada.

desenvolvimento de aplicativos em contêineres. A operadora também tem a opção de trabalhar com o fornecedor para determinar e influenciar seus processos de CI/CD; e de proteção da chave criptográfica NG-RAN (KgNB), que é armazenada no CU, localizado em um *data center* centralizado dentro da rede.

Porém, cumpre ressaltar que o relatório do BSI citado anteriormente menciona existência de vulnerabilidades em uma rede aberta em operadores de nuvem, em operadores da RAN, em diversas interfaces, em rApps (microsserviços extensíveis de terceiros contidos no *Non Real Time* RIC), em xApps e nas ferramentas de *machine learning*.

6.2.5. ZTA em *Kubernetes*

Kubernetes, um sistema de orquestração *open-source* que automatiza a implantação, o dimensionamento e a gestão de aplicações em contêineres, fornece vários recursos de segurança integrados para proteger este ambiente, incluindo segurança de rede, isolamento de recursos, controle de acesso, registro e auditoria. Alguns dos controles integrados comuns de *Kubernetes* que ajudam a aumentar a segurança incluem:

- RBAC no *cluster* (um conjunto de nós que executam aplicativos em contêineres), que fornece uma estrutura para implementar o princípio de privilégio mínimo para humanos e aplicativos que acessam a API *Kubernetes*.

- Configuração de contexto de segurança para *pods* (grupo de componentes conteinerizados) para limitar suas capacidades.

- Política de segurança do *pod*, que define padrões de como as cargas de trabalho podem ser executadas no *cluster*. Esses controles podem eliminar classes inteiras de ataques que dependem de acesso privilegiado.

- Uso de políticas de rede de *Kubernetes* para controlar o tráfego entre *pods* e *clusters*.

- Políticas de rede de *Kubernetes* que permitem o controle do acesso à rede para dentro e para fora dos aplicativos em contêineres. Além desse recurso, *firewalls* baseados em *software* podem ser implantados para controlar a comunicação de contêiner para contêiner dentro ou entre diferentes *clusters*.

- Uso de *namespaces* para isolar cargas de trabalho confidenciais e criar limites de segurança. Separar cargas de trabalho em *namespaces* pode ajudar a conter ataques e limitar o impacto de erros ou ações destrutivas de usuários autorizados.

- Avaliação de privilégios do contêiner; aderir ao princípio do menor privilégio e fornecer os privilégios e recursos mínimos que permitiriam ao contêiner desempenhar sua função pretendida.

- Uso de *Transport Layer Security* (Segurança no nível de transporte, TLS) mútuo para todas as comunicações entre *clusters* e intra *clusters*.

- Capacidade de criptografar o armazenamento de dados etcd[45] (um armazenamento de valor-chave distribuído que fornece uma maneira de armazenar dados) para proteger a infraestrutura e segredos do aplicativo ou para oferecer suporte à integração com cofres externos.

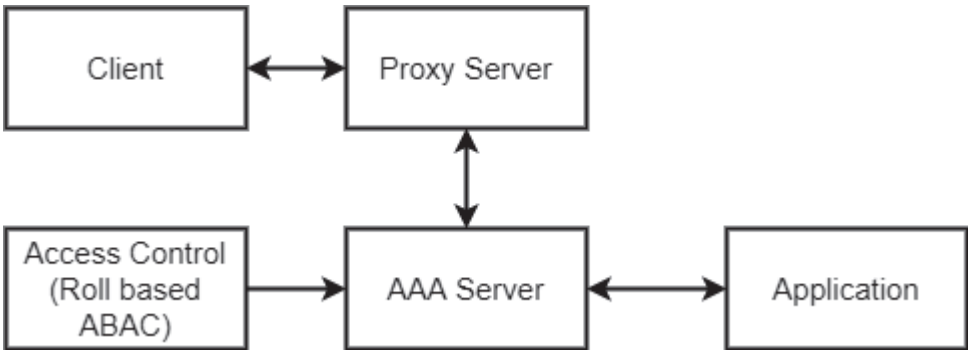

Figura 14 – diagrama em blocos de arquitetura *Zero Trust*[46]

A abordagem tradicional de segurança, baseada em um perímetro, possui vulnerabilidades conforme anteriormente detalhado. A abordagem *Zero Trust* pode ser adequada para serviços baseados em nuvem e segurança de rede dentro de uma organização, uma vez que não possui confiança a priori em serviços e aplicativos. Uma estratégia *Zero Trust* impõe controle de acesso estrito e específico para aumentar a segurança na nuvem, enquanto mantém registros ou logs de todas as atividades na rede. A Figura 14 – diagrama em blocos de arquitetura *Zero Trust* mostra a visão geral da arquitetura do sistema. O cliente se conecta ao servidor *proxy*, cuja configuração o torna um *proxy* reverso, impedindo o usuário de saber o endereço IP real do servidor de autenticação e autorização. O servidor *proxy* então redireciona o cliente para o servidor de autenticação e autorização. O controle de acesso decide se o usuário tem permissão de acesso ao aplicativo. Se ele for autenticado, terá autorização para acessar o aplicativo. O servidor de autenticação e autorização verifica continuamente os certificados para garantir que nenhum usuário comprometido entre ou se mantenha no sistema.

O servidor *proxy* é responsável por enviar a requisição do cliente para o *cluster Kubernetes*. O servidor de autenticação e autorização é o único mediador entre o servidor *proxy* e o aplicativo. É nele onde se encontra *Kubernetes*, que gerencia serviços e aplicações conteinerizados. O bloco de controle de acesso fornece um atributo específico dentro da autoridade que o usuário possui na organização. O aplicativo é armazenado no cluster *Kubernetes*, junto a outros em uma máquina virtual. No entanto,

[45] etcd (https://etcd.io/) é um armazenamento de chave/valor *open source*, distribuído e consistente para configurações compartilhadas, descoberta de serviços e coordenação do agendador de sistemas distribuídos ou clusters de máquinas.
[46] D. D'Silva and D. D. Ambawade, "*Building A Zero Trust Architecture Using Kubernetes*," 2021 6th International Conference for Convergence in Technology (I2CT), 2021, pp. 1-8, doi: 10.1109/I2CT51068.2021.9418203.

eles estão conectados a *Kubernetes* por meio de *tokens* ao portador atribuídos permanentemente, tornando-os escravos do nó mestre.

Zero Trust introduz um novo paradigma de segurança com políticas rígidas para garantir que nenhum ativo permaneça comprometido. A infraestrutura existente aparenta ser inadequada devido à possibilidade de se obter acesso privilegiado. *Zero Trust* depende de uma combinação de controles de acesso, garantindo dificuldade de invasão.

Atualmente há uma gama de ativos, desde aplicativos até autenticação, em desenvolvimento em contêineres. Logo, a infraestrutura deve ser desenvolvida de acordo para evitar o isolamento destes. Porém, a estrutura física, como *firewalls* e servidores *proxy* também são necessários para garantir a segurança de rede.

6.2.6. Avaliação de segurança em processos produtivos

NESAS – *Network Equipment Security Assurance Scheme* – é uma iniciativa voluntária da indústria móvel para lançar um programa contínuo de melhoria de segurança com foco em equipamentos de infraestrutura de rede móvel. O NESAS abrange equipamentos projetados para suportar funções definidas pelo 3GPP que são implantados por operadoras móveis em suas redes. O NESAS consiste em avaliações de segurança dos processos de desenvolvimento do fornecedor e do ciclo de vida do produto e de segurança de produtos de rede, que definem um nível de segurança básico para a indústria.

Além de fornecedores mais tradicionais do mercado de telecomunicações, o primeiro *player OpenRAN* a alcançar tal acreditação foi a Mavenir, que a recebeu sobre solução de acesso virtualizada, que inclui CU e DU, núcleo de rede em nuvem e soluções nativas em nuvem. Os demais entes que possuem a acreditação NESAS são Huawei, ZTE, Nokia, Ericsson e Samsung[47].

6.2.7. Segurança – Conclusão

Como visto, há preocupações concretas de que a abordagem atualmente utilizada para garantia de segurança em redes de acesso, baseada em confiança nos procedimentos, controle de acesso de usuário e defesa de perímetro, não seja apropriada para as redes atuais, em especial *OpenRANs*. Como estas são mais abertas do que as RANs monolíticas e, a princípio, podem possuir mais superfície de ataque, a sua política de segurança deve garantir que possíveis vulnerabilidades sejam expostas e tratadas a contento.

Nesta seção foi exposta uma abordagem, *Zero Trust Architecture*, que pode ser mais apropriada para redes com diversas fragilidades possíveis, como IoT (internet das coisas), BYOD e grande número de interfaces, para citar algumas. Porém, ZTA não é a

[47] https://www.gsma.com/security/nesas-participating-vendors/

única iniciativa atualmente em estudos, podendo ser mencionadas *blockchain* RAN[48] (B-RAN), *decryption of network traffic*[49], entre outras, que pretendem aumentar a segurança de redes de acesso.

Não obstante, importante ressaltar a relevância do papel de iniciativas que procuram estabelecer níveis mínimos de segurança em redes e equipamentos, como o NESAS, que investiga e certifica o nível de segurança da infraestrutura de telecomunicações. Desta forma, por mais que ameaças de segurança cibernética estejam presentes tanto em redes de acesso legadas e proprietárias quanto em abertas, as ações do mercado e o desenvolvimento de novas tecnologias permitem que a segurança em redes de acesso possa se manter em um nível apropriado para atendimento das atuais demandas de telecomunicações e para as que se apresentam, com grande densidade de dispositivos e diversidade de fornecedores.

Outra iniciativa em andamento é a avaliação pela Anatel de possível esquema, que não se confunde com certificação ou homologação de equipamentos, de acompanhamento de processos industriais para garantia de segurança em fornecedores que pretendem vender para operadoras no Brasil, em confluência com o artigo 7º do Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações, aprovado pela Resolução nº 740, de 21 de dezembro de 2020.

6.3. Subgrupo 2 – Aspectos Econômicos – Potenciais Ganhos Econômicos com *OpenRAN*

É certo que um dos fatores que sopesará para que as prestadoras de serviços de telecomunicações incorporarem em suas redes equipamentos *OpenRAN* será o econômico. Já existem estudos que remontam que a adoção de equipamentos *OpenRAN* na rede de telecomunicações poderá gerar economias de até 30% (trinta por cento), conforme seção Topologias e *splits*.

Conforme já discorrido anteriormente, a tecnologia 5G, por se utilizar de frequências mais altas, necessitará de mais antenas para garantia a cobertura do serviço a seus usuários, assim se equipamentos com tecnologia *OpenRAN* proporcionarem uma economia de investimento e de operação para as prestadoras, as economias podem ser ainda maiores.

Um aspecto importante que se deve levar em consideração é que o sucesso da topologia *OpenRAN* depende, dentre diversos fatores, da manutenção de uma comunidade diversa e ativa de fornecedores, com oportunidade de negócios para todos dentro do ecossistema de soluções de rede. No longo prazo, isso pode se tornar um desafio, pois fornecedores menores e instáveis economicamente podem ter maiores dificuldades para manterem-se ativamente no mercado.

[48] X. Ling, J. Wang, T. Bouchoucha, B. C. Levy and Z. Ding, "*Blockchain Radio Access Network (B-RAN): Towards Decentralized Secure Radio Access Paradigm*," in *IEEE Access*, vol. 7, pp. 9714-9723, 2019, doi: 10.1109/ACCESS.2018.2890557.
[49] https://threatpost.com/decryption-improve-security/176613/

Em 2021 houve notícias de que Rakuten, Dish, Telefônica e Vodafone estão implementando em suas redes equipamentos com tal tecnologia, assim cumpre observar dos relatos destas empresas se efetivamente ocorreram economias na construção das redes de telecomunicações.

6.3.1. Custos da Rede

TCO é um parâmetro importante para as redes móveis. Os prestadores de serviços de telecomunicações móveis se baseiam neste para saber quanto custará a rede para a prestação do serviço e, em geral fundamentado nisso, estabelecem o valor de custo e o valor a ser tarifado do usuário.

Em geral o TCO de uma empresa de telecomunicações engloba Capex e Opex, que segundo consultorias internacionais apresentariam a divisão explicitada na Figura 15 - Exemplo de Capex de empresa de telecomunicações e na Figura 16 - Exemplo de Opex de empresa de telecomunicações[50]:

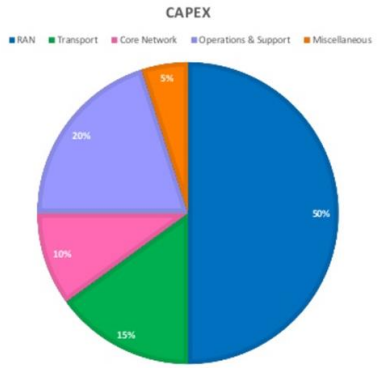

Figura 15 - Exemplo de Capex de empresa de telecomunicações

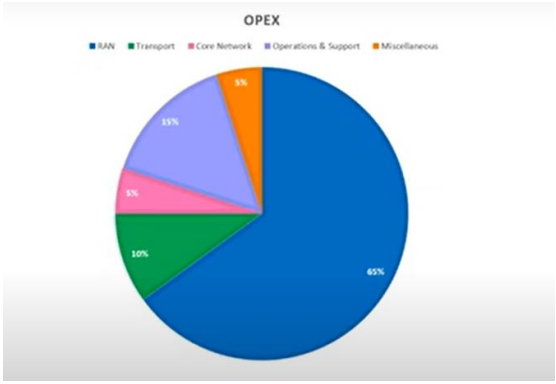

Figura 16 - Exemplo de Opex de empresa de telecomunicações

[50] https://blog.3g4g.co.uk/2020/10/understanding-tco-of-mobile-network.html

Verifica-se na Figura 15 - Exemplo de Capex de empresa de telecomunicações que a RAN representaria 50% do Capex e, na Figura 16 - Exemplo de Opex de empresa de telecomunicações, 65% do Opex. Neste sentido, vale a pena esmiuçar os atuais custos da RAN Capex e Opex[50].

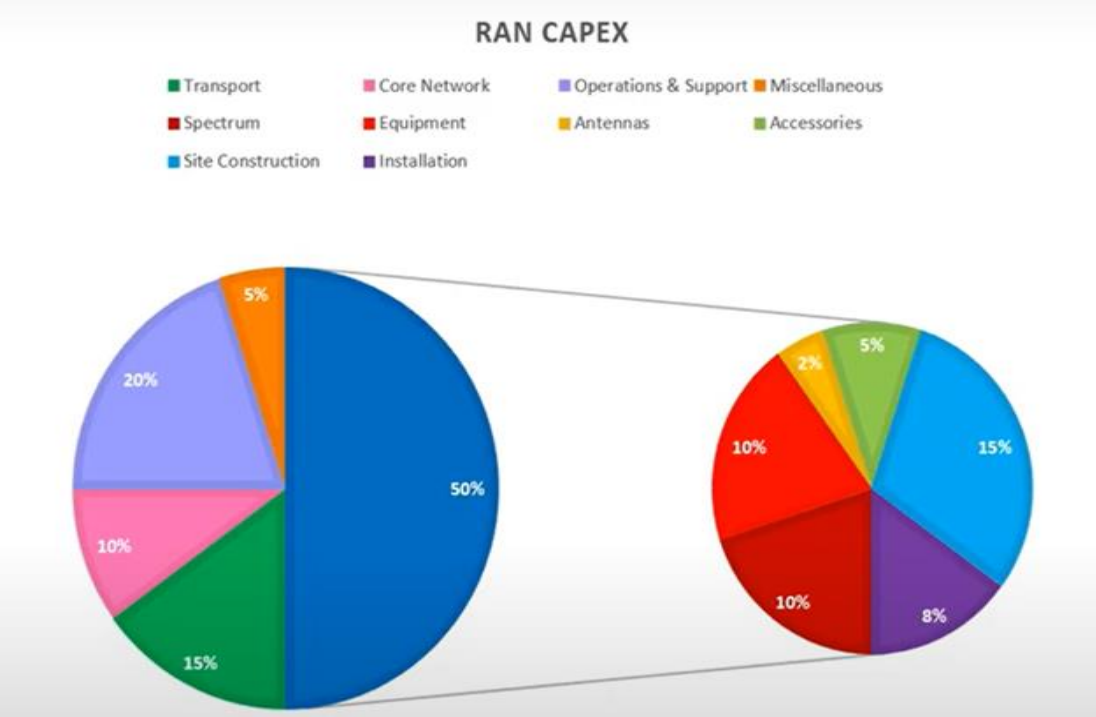

Figura 17 - Detalhamento do Capex de RAN

Estudos concluíram que RAN aberta pode reduzir o Capex em 40% a 50% e as despesas operacionais em 30% a 40% em relação a uma configuração de rede móvel celular tradicional[51]. A maioria desses estudos cita a Rakuten, que está se esforçando para construir a primeira e maior rede nativa em nuvem virtualizada ponta a ponta usando arquiteturas *OpenRAN*.

[51] https://www2.deloitte.com/xe/en/insights/industry/technology/technology-media-and-telecom-predictions/2021/radio-access-networks.html

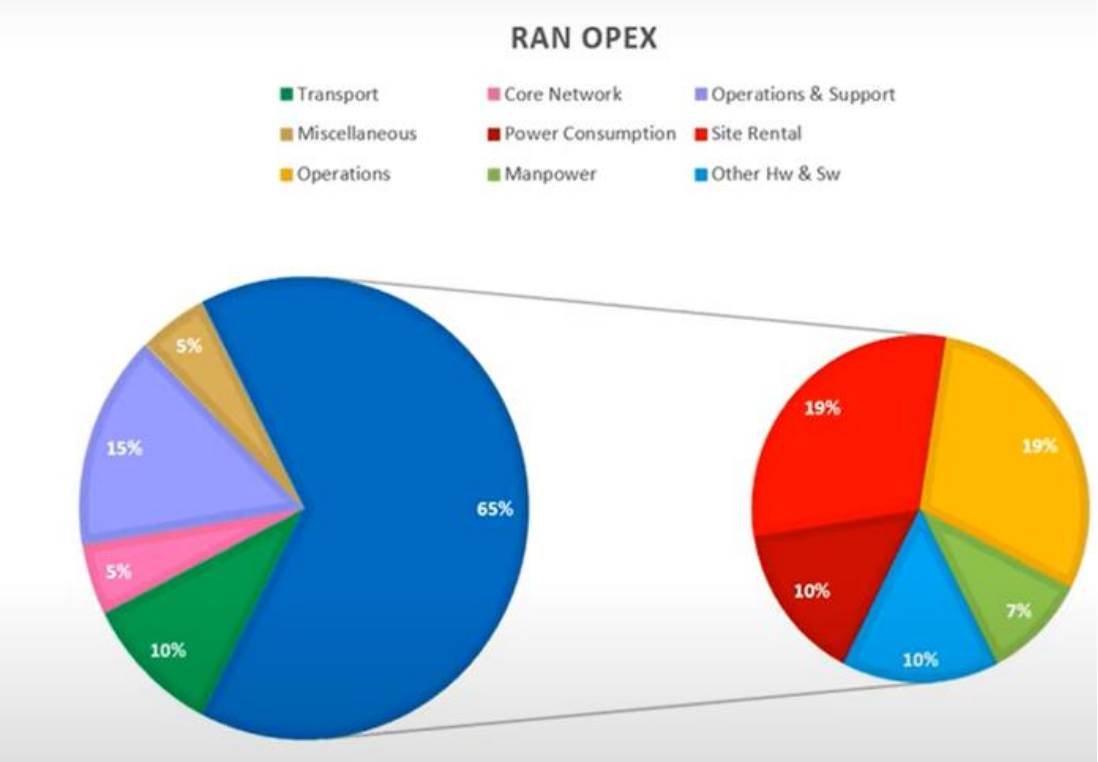

Figura 18 - Detalhamento do Opex de RAN

Acredita-se que o maior ganho econômico que se pode ter na parte de equipamentos no Capex está justamente na virtualização da rede, que além de diminuir equipamentos a serem monitorados ocupam menos espaço na torre, fator que influencia diretamente no custo do aluguel (Figura 19 - Ganhos de Capex com a virtualização da RAN). A topologia *OpenRAN* nesse sentido permitiria a redução com a existência de diversidade de fornecedores e que podem ser diversos dos que fornecem o *hardware*. Um maior número de fornecedores, além de aumentar a concorrência, que de regra diversifica os equipamentos disponíveis no mercado, reduz o tempo de sua disponibilização e reduz os preços médios e pode reduzir o tempo de inovação.

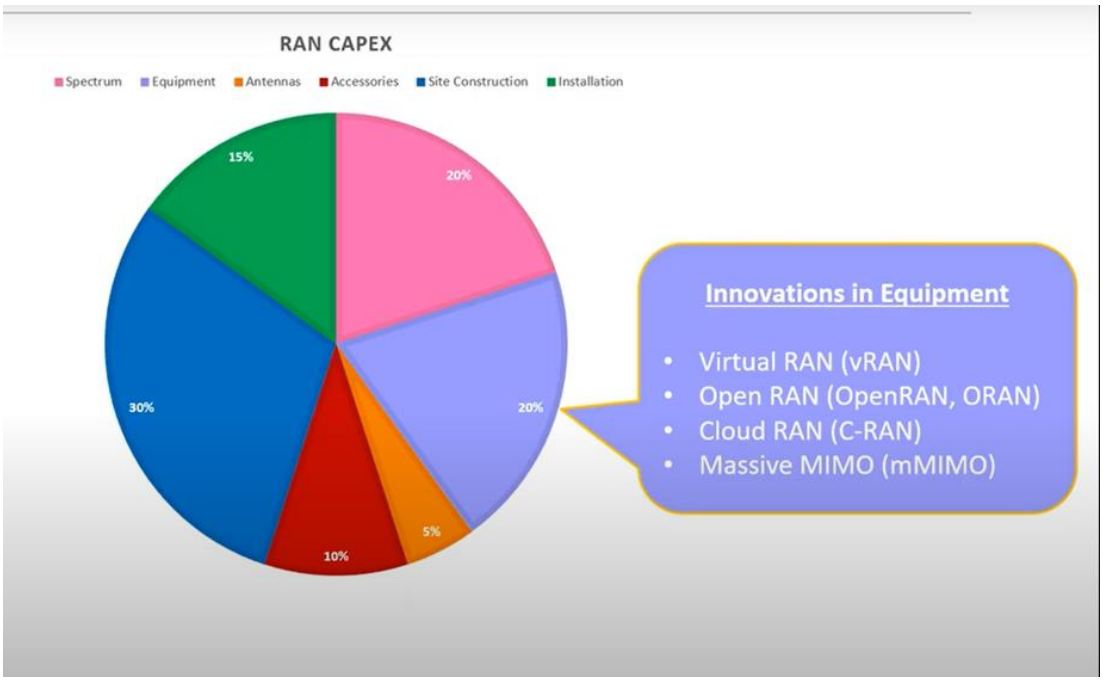

Figura 19 - Ganhos de Capex com a virtualização da RAN

Na Figura 20 - Ganhos de Opex com a virtualização da RAN verifica-se que a topologia *OpenRAN* pode impactar reduzindo o Opex, já que induziria a maior automatização da rede com inteligência artificial e *machine learning*. A virtualização da rede, assim, diminuiria a dependência de um único fornecedor, podendo reduzir os custos de manutenção e operacionalização.

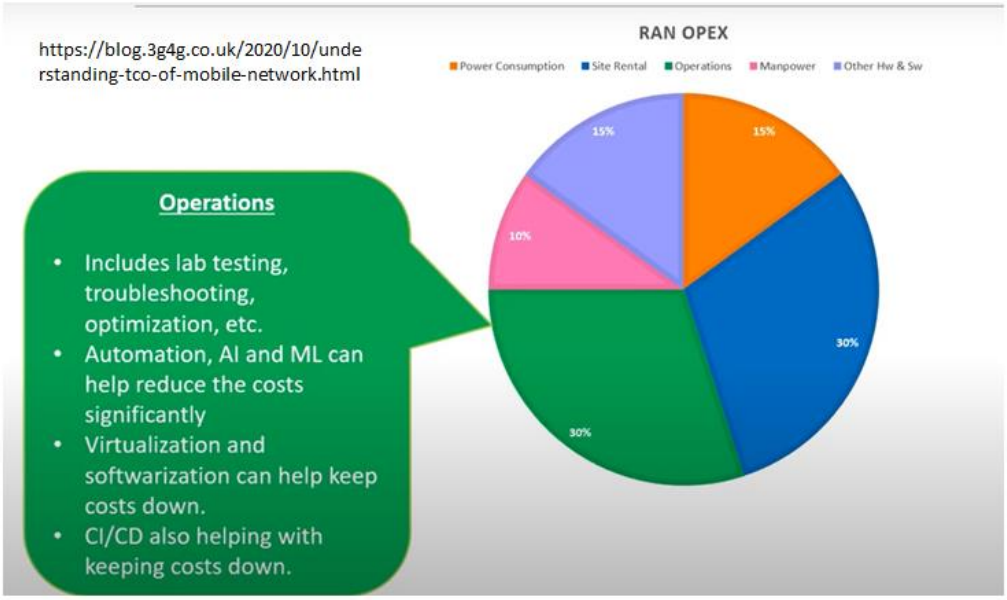

Figura 20 - Ganhos de Opex com a virtualização da RAN

Os operadores podem usar *software* para atualizar os recursos e funcionalidades de RAN na mesma infraestrutura física para acompanhar as mudanças nas condições do mercado, em vez de ter que eliminar e substituir sistemas físicos inteiros. Outro ponto é a ampliação da concorrência de fornecedores, que pode reduzir ainda mais os custos de *hardware*. Deste modo, a topologia *OpenRAN* permite que as operadoras escolham entre os fornecedores – não apenas fornecedores de telecomunicações tradicionais, mas grandes empresas de tecnologia, como fabricantes de *hardware*, *webscalers*, fabricantes de *design* original e outros que procuram entrar no mercado. Verifica-se que empresas como AWS e Intel, dentre outras, estão cada vez mais interessadas em prover soluções às redes de telecomunicações.

Em questões de quantitativo, um estudo da *Mobile Experts*[52] demonstra que os ganhos no Opex estariam na redução do backhaul e nos custos dos equipamentos, conforme Figura 21 - Ganhos de Opex no *backhaul*.

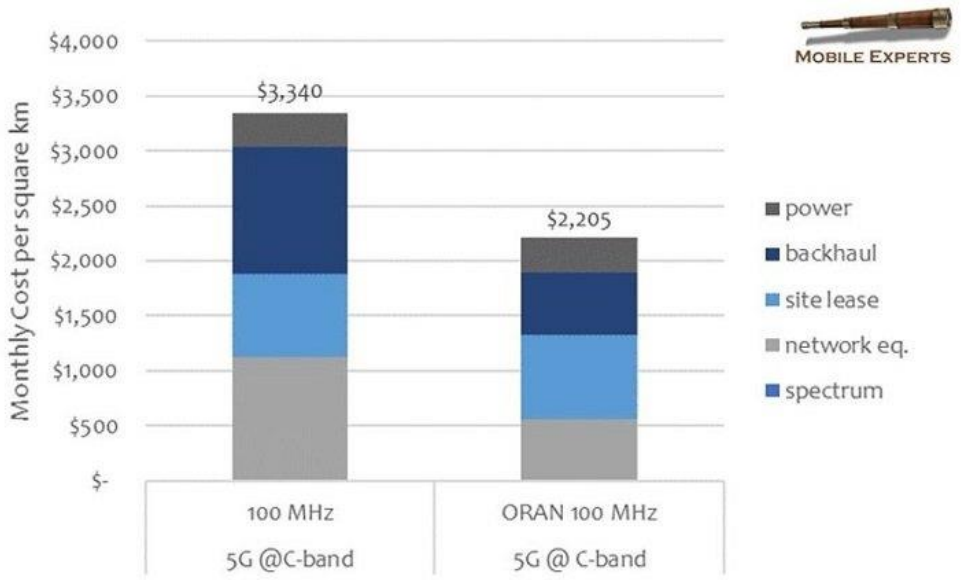

Figura 21 - Ganhos de Opex no *backhaul*

Aplicado o modelo de rede aberta em ambientes urbanos, segundo o estudo da *Mobile Experts*, ainda não haveria ganho em relação ao modelo proprietário. Em que pese os custos de equipamentos sejam menores, o aluguel do site e valor do espectro se apresentam maior em relação ao modelo de rede proprietário conforme Figura 22 - Custos de RAN vs. *OpenRAN* em ambiente urbano.

[52] https://www.fiercewireless.com/tech/industry-voices-madden-oran-really-cheaper

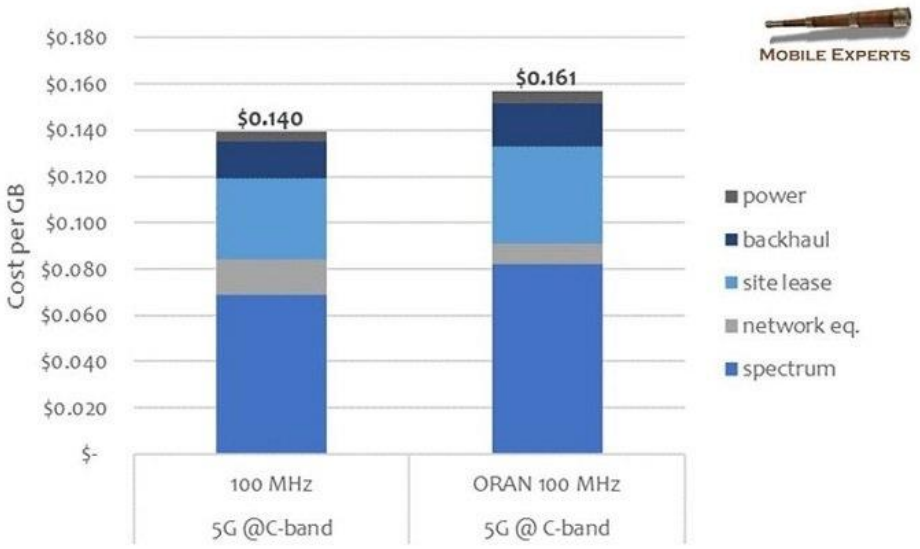

Figura 22 - Custos de RAN vs. *OpenRAN* em ambiente urbano

Segundo a ACG *Research*[53], os cenários de análise de TCO mostram que uma rede aberta tem os seguintes benefícios financeiros em relação a uma proprietária:

> As redes de acesso via rádio abertas serão 30% mais baratas do que as proprietárias atualmente disponíveis ao longo do tempo. Isto porque haverá mais fabricantes desenvolvendo uma especificação de rádio padronizada. Espera-se que as margens de lucro sejam menores para redes abertas, fabricadas por *white-box vendors* (fabricantes de soluções generalistas), do que os rádios proprietários atualmente disponíveis.
>
> O *software* de RAN aberta será 30% mais barato do que o *software* proprietário atualmente disponível ao longo do tempo. Isso é resultado de uma combinação de fornecedores de *software* de código aberto e vários fornecedores em um ecossistema aberto.
>
> Os servidores x86 acabarão se tornando mais baratos que as BBUs proprietárias. Este é o resultado da *Moore's Law*[54] e as melhorias contínuas nos processadores generalistas projetados para os requisitos de *OpenRAN*.

A ressalva realizada pela ACG é que, embora as declarações de custo total de propriedade possam ser válidas em operadoras que estão construindo a rede, como no esforço da Rakuten, essa magnitude de economia de custos parece altamente

[53] https://acgcc.com/media/uploads/2021/05/19/acg-the-economic-benefits-of-open-ran-technology.pdf

[54] Lei de Moore é uma expressão usada para se referir à observação feita por Gordon E. Moore sobre a tendência histórica da indústria de microchips e processadores. Segundo ela, o número de transistores dos chips teria um aumento de 100%, pelo mesmo custo, a cada dois anos.

improvável em grandes operadoras, onde investimentos significativos já foram feitos. Consequentemente, as operadoras que buscam adotar RAN aberta em infraestruturas existentes precisariam substituir o equipamento legado, o que aumentaria significativamente o custo geral de implantação de uma RAN aberta[51]. Deve-se ainda ressaltar que, para as prestadoras com rede já construída, *OpenRAN* também altera o modo de gestão de redes, já que pressupõe um modelo de gerenciamento com automação e inteligência artificial, se aproximando do estilo TI e engenharia de *software*. As inovações na rede também serão mais contínuas com novos aplicativos que permitam maior velocidade e previsão da operação.

Quanto ao montante dispendido pelas prestadoras, se baseando nos dados divulgados pela Dell'Oro *Group*[55], empresa de consultoria, os gastos anuais em redes de acesso de rádio normalmente chegam a valores entre US$ 30 bilhões a US$ 35 bilhões por ano, enquanto o Capex de redes sem fio em geral chega a US$ 150 bilhões. Verifica-se que boa parte do referido valor vai para infraestrutura física, como torres, aço e cimento, que não pode ser simplesmente virtualizada ou transformada em *software*.

Outros estudos, a exemplo do da *Strand Consult*[56], os gastos com redes de acesso de rádio representam 2,8% e 3,6% da ARPU de telecomunicações (*average revenue per user*, receita média por usuário), portanto a economia trazida por *OpenRAN* seria apenas de 1% da ARPU. No Brasil estima-se que a ARPU de telecomunicações esteja varia de R$ 13 no pré-pago e R$ 33 no pós-pago, conforme Figura 23 - ARPU SMP pré e pós no Brasil.

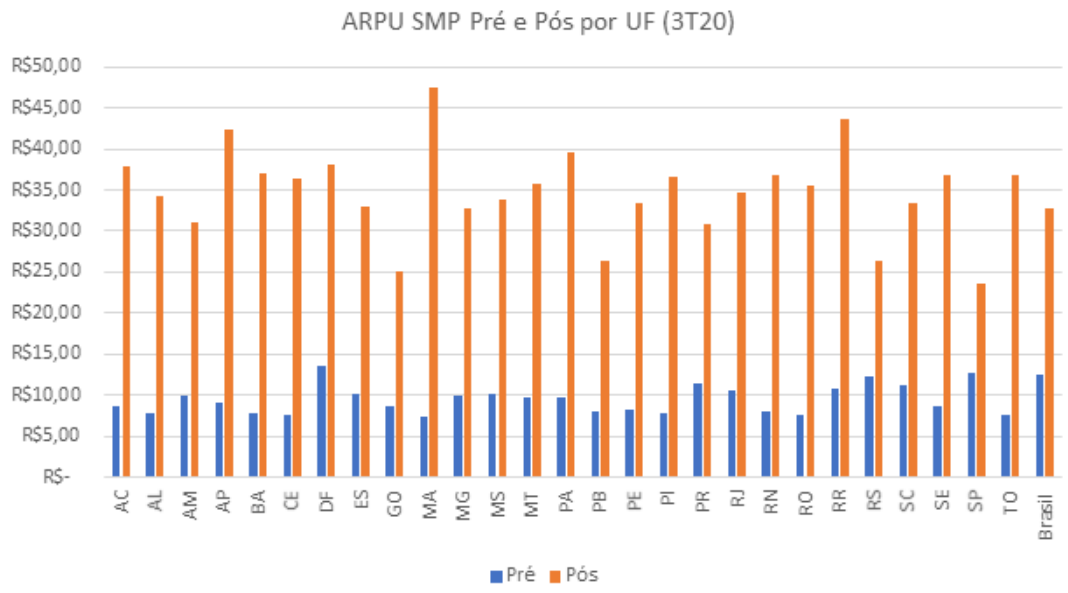

Figura 23 - ARPU SMP pré e pós no Brasil

[55] https://www.lightreading.com/open-ran/open-ran-and-everest-of-inflated-expectations/a/d-id/764850
[56] https://techblog.comsoc.org/2022/01/24/strand-consult-open-ran-hype-vs-reality-leaves-many-questions-unanswered/

Os estudos mais conservadores entendem as economias advindas da diversidade de fornecedores são teóricas. Muitos especialistas do setor argumentam que o custo, o tempo e o esforço adicionais para testar e integrar sistemas de vários fornecedores podem compensar, se não anular completamente, quaisquer benefícios da diversidade de fornecedores[51]. Além disso, o desempenho dos recursos de RAN de processamento intensivo em *hardware* de uso geral pode não corresponder ao que pode ser alcançado em plataformas de *hardware* otimizadas sob medida.

Uma das *features* que tem trazido certa segurança na promissora aplicabilidade da arquitetura *OpenRAN* é que muitas operadoras mundiais têm demonstrado interesse ou já tem adicionado equipamentos abertos a sua rede, dentre elas pode-se citar a AT&T, Vodafone, Dish Network, British Telecom, Orange, Deutsche Telekom, NTT DoCoMo, Reliance Jio, SK Telecom, Telus, TIM, Turkcell, Verizon, MTN, Orange, Etisalat e algumas empresas *tier* 2 e 3 nos EUA. O Dell'Oro *Group* prevê que, até 2024, as operadoras gastarão algo acima de US$ 3 bilhões em produtos *OpenRAN*, o que representa uma participação de dois dígitos no mercado nos próximos cinco anos.

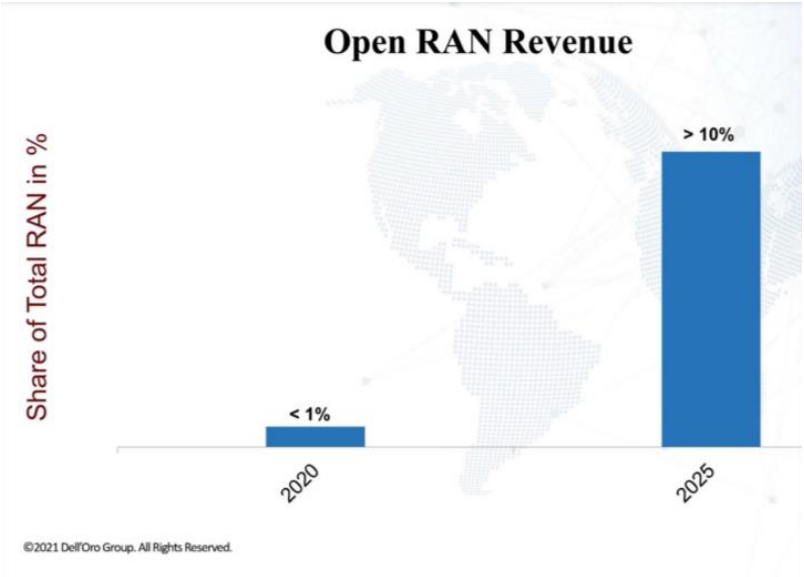

Figura 24 - Receita *OpenRAN*

Nesse mesmo sentido, a ABI *Research*[57] prevê que, para redes externas públicas, as vendas de produtos *OpenRAN* atingirão US$ 40,7 bilhões, ou 45% de participação, até 2026. Esses números incluem taxas de aluguel de torre e despesas trabalhistas.

[57] https://www.abiresearch.com/press/open-ran-radio-units-soar-more-us47-billion-2026/

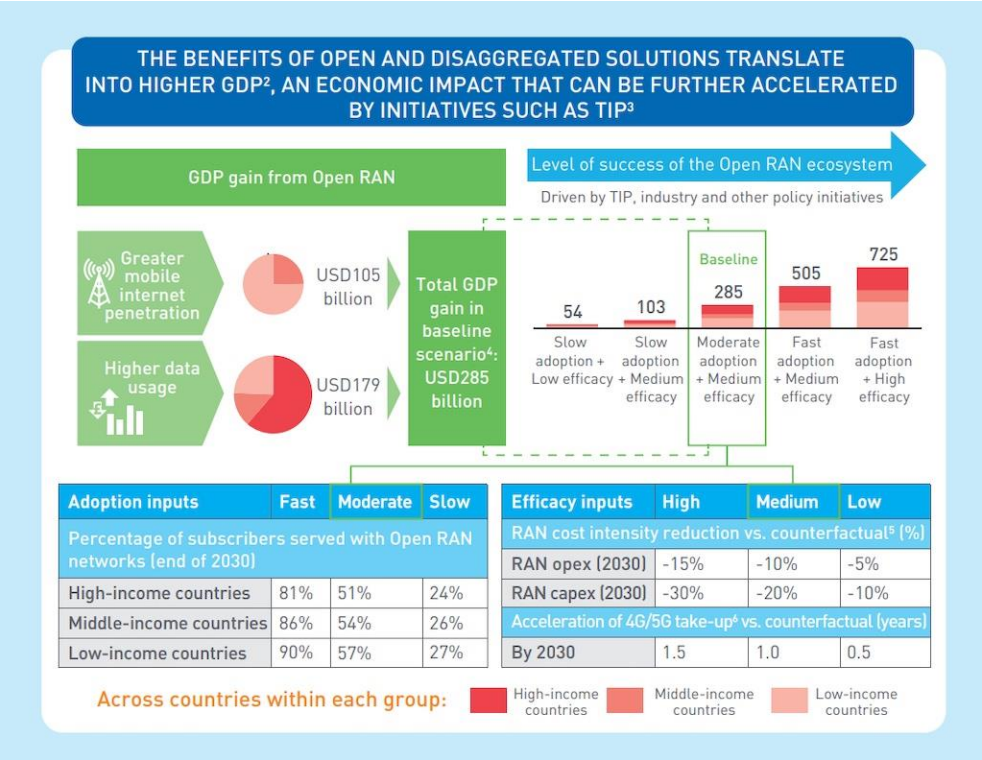

Figura 25 - Benefícios *OpenRAN* e impactos econômicos

Segundo relatório da Analysys Mason[58], as receitas da arquitetura *OpenRAN* possivelmente teria a configuração apresentada na Figura 26 - Configuração de receitas *OpenRAN*:

[58] https://www.analysysmason.com/research/content/reports/open-ran-framework-rma18/

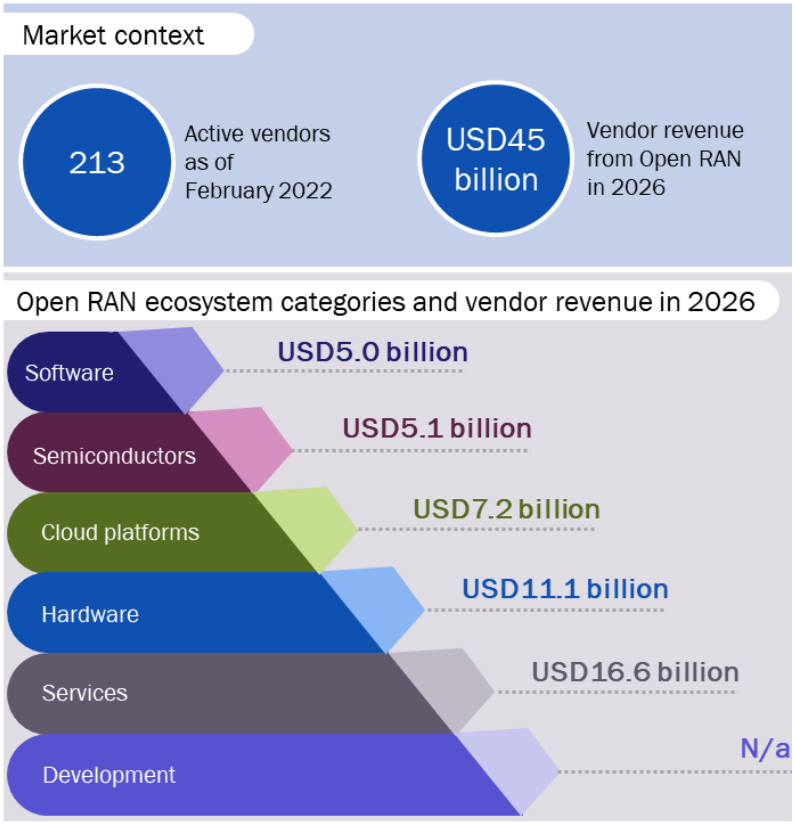

Figura 26 - Configuração de receitas *OpenRAN*

Segundo o relatório da *Mobile Experts*[59], o mercado de RAN está crescendo a uma taxa anual composta (CAGR) de 3%, com −1% de crescimento em macro estações base e 25 a 35% em segmentos de ondas milimétricas e *software*.

Verifica-se da Figura 26 - Configuração de receitas *OpenRAN* que em todos os cenários há perspectivas para sucesso do desenvolvimento da arquitetura *OpenRAN* para redes móveis. Deste modo, cabe analisar alguns casos mundiais.

6.3.2. Estudos de casos mundiais

Há diversos cases mundiais que estão implantando equipamentos *OpenRAN* em suas redes, conforme Figura 27 - Casos de uso mundiais de redes abertas:

[59] https://www.lightreading.com/5g/ericsson-clocked-as-number-one-in-ran-market---mobile-experts/d/d-id/774853

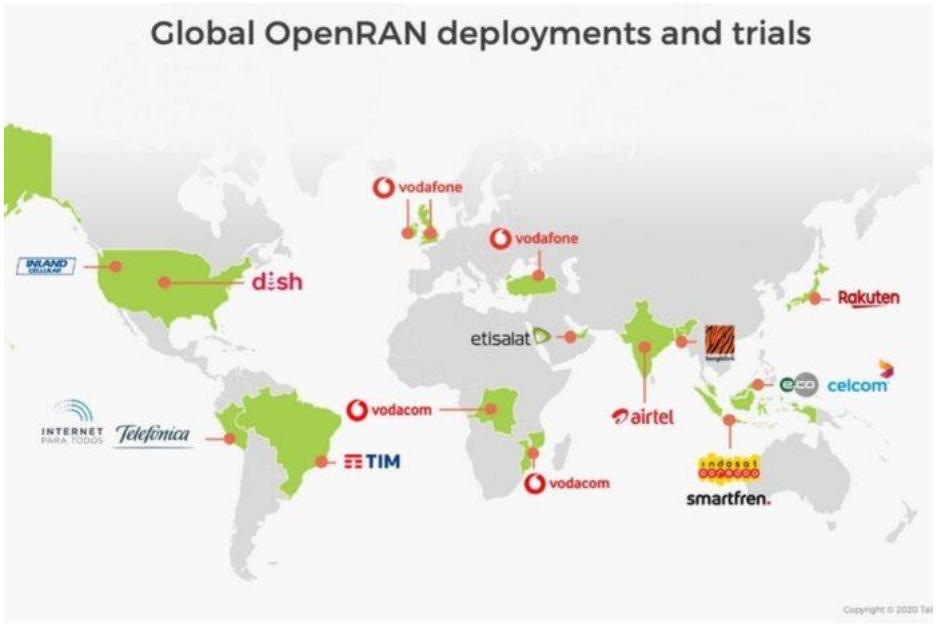

Figura 27 - Casos de uso mundiais de redes abertas

O caso mais comentado é da operadora japonesa Rakuten, que implementou 30.000 sites, em outubro de 2021, com equipamentos *OpenRAN*[51]. Por se tratar de uma operadora entrante, especialistas têm dito que a falta de infraestrutura legada ajuda a reduzir o risco e o custo de implantação. Recentes relatórios sobre a adoção de arquitetura de rede aberta têm atribuído uma economia de 40% dos custos de implementação em relação a contratação de estrutura proprietária tradicional.

No Estados Unidos, um dos principais cases é da Dish *Network* para a construção de sua rede 5G *greenfield* com infraestrutura de rede aberta. A Dish está fazendo parceria com inovadores de eletrônicos, nuvem e telecomunicações dos EUA, como Qualcomm, Dell Technologies, IBM, Intel e Mavenir para construir sua rede. A empresa visa construir uma rede nacional *OpenRAN* até 2023 que cubra 70% da população dos EUA. Nesse sentido, estima-se que já tenha gastado mais de US$ 10 bilhões em sua infraestrutura e está construindo redes finais em 42 áreas urbanas.

A Vodafone tem realizado diversos testes de RAN aberta no Reino Unido, África do Sul, Moçambique, Turquia, Irlanda e República Democrática do Congo, com grandes expansões de rede com equipamento de rede aberta. Em janeiro de 2022, implantou a primeira ERB com RAN aberta na Inglaterra, com uma projeção de instalação de mais de 2.500 unidades até 2027. Os fornecedores de equipamento serão a Dell, NEC, Samsung *Electronics*, Wind River, Capgemini *Engineering* e Keysight *Technologies*. Samsung será o fornecedor de *software* RAN de referência. A Samsung e a NEC fornecerão o *Massive* MIMO juntamente com as unidades de rádio Samsung e Evenstar, que estabelecem um sinal entre os *smartphones* ou dispositivos dos usuários e a antena. Os rádios Evenstar fazem parte de um esforço conjunto entre o Facebook e a Vodafone para criar unidades de rádio *white-box* dentro do Telecom Infra Project (TIP) e são um componente chave para a iniciativa.

As implantações iniciais serão realizadas usando servidores COTS Dell EMC *PowerEdge* para oferecer suporte à função combinada DU/CU executando o *software*

Containers as a Service (CaaS) do Wind River Studio, que fornecerá uma plataforma de hospedagem distribuída nativa em nuvem aos aplicativos *OpenRAN* e vRAN da Samsung, o que conferirá à Vodafone o benefício de poder misturar, combinar e instalar novas versões e atualizações de *software* com mais facilidade.

A Orange implantou uma rede experimental com parceiros de tecnologia como Mavenir, HPE, Dell Technologies e Xiaomi. Como projeto, a Orange também desenvolveu o "*Orange Open RAN Integration Center*" localizado em Orange Gardens, Châtillon, perto de Paris. O laboratório estará disponível a fornecedores de equipamentos do ecossistema *OpenRAN*, *sstartups* e integradores de sistemas que pretendam testar o funcionamento e interoperabilidade dos seus componentes com os de outros fornecedores e visa permitir, a longo prazo, a implantação de redes capazes de trabalhar com *hardware* e *software* de diferentes fornecedores. A operadora, presente em 26 países, se comprometeu a implantar estações com a arquitetura *OpenRAN* a partir de 2025. Provavelmente a operadora iniciará as implantações em áreas rurais, redes internas e privadas.

A espanhola Telefônica anunciou que realizou testes de tecnologia RAN aberta 4G e 5G na Alemanha, Espanha, Reino Unido e Brasil em 2020, juntamente com a NEC. No Brasil o teste foi realizado em Juazeiro e Petrolina. A Telefônica também tem projetos de redes abertas no Peru. Espera-se como resultado possuir redes mais flexíveis, eficientes e seguras na era 5G.

Além disso, a NEC e a Telefônica continuam com a parceria para validar e implementar tecnologias *OpenRAN* e casos de uso no Laboratório de Tecnologia e Automação da Telefónica, criado recentemente na Espanha. Já o Centro de Excelência Global *OpenRAN* da NEC, no Reino Unido, conduzirá a aprovação de fornecedores e o desenvolvimento conjunto de casos. Conforme notícias, as soluções *OpenRAN* são compostas por um ecossistema de produtos próprios da NEC, bem como produtos de *software* e *hardware* de parceiros. As unidades de rádio mMIMO (*massive* MIMO, MIMO maciço) 5G aberto da NEC com *beamforming* avançado que ajuda significativamente a aumentar/otimizar a capacidade da rede farão parte do ecossistema. Os casos de uso terão RICs orientados por inteligência artificial buscando a otimização de RAN, a automação do ciclo de vida do serviço com base em SMO, automação de teste e implantação de acordo com CI/CD da Telefónica, bem como a otimização da economia de energia.

Em 2022, a Telefônica validou uma *smallcell* com tecnologia *OpenRAN* composta de equipamento e *software* de múltiplos fornecedores com tecnologia 5GSA, sendo a antena de *smallcell* desenvolvida pela empresa Askey, os processadores pela Qualcomm, e os rádios de acesso, segurança e *software* pela Node-H. A Vivo ainda constatou que a tecnologia também poderá ser aplicada as *macrocells* e na construção de redes privativas.

A Deutsche Telekom constituiu um Centro Europeu de Teste e Integração para testar soluções compatíveis com RAN aberta programável e desagregada. A Deutsche Telekom tem como um de seus projetos, em Neubrandenburg, a "O-RAN Town", que terá uma rede 4G e 5G em até 25 locais com equipamentos *OpenRAN*. Os primeiros

locais já estão operacionais e integrados à rede da prestadora. Trata-se da primeira integração da Europa de unidades de rádio mMIMO, que são conectadas ao *software* da RAN virtualizada por meio do *fronthaul* aberto. Assim, a Deutsche Telekom está desenvolvendo o SMO como o núcleo para o gerenciamento do ciclo de vida completo (LCM) de todos os componentes *OpenRAN*.

Os primeiros locais ativos da O-RAN Town são baseados em uma arquitetura RAN aberta de vários fornecedores. As unidades de rádio remotas são fornecidas pela Fujitsu e pela NEC, incluindo as unidades de rádio LTE e 5G NR da Fujitsu e as unidades de rádio 5G mMIMO da NEC que fornecem as especificações do *fronthaul* e apresentam tecnologias avançadas de formação de *beamforming*. A nuvem de banda base nativa para as DUs, CUs e RUs 4G e 5G foram obtidas da Mavenir. O *hardware* de servidor padrão é fornecido por Dell e Supermicro. Toda a arquitetura de nuvem *OpenRAN* é construída na arquitetura de *software* Intel FlexRAN.

A Etisalat, um provedor de serviços de telecomunicações com sede nos Emirados Árabes Unidos, está lançando a primeira RAN virtual do Oriente Médio em colaboração com os principais fornecedores de tecnologia de RAN. Sua solução busca desacoplar os elementos programáveis do *software* RAN do *hardware*. Isso permitiria que o *hardware* e as plataformas de servidor geralmente disponíveis processassem o *software* RAN, melhorando a flexibilidade de implantação, escalabilidade, agilidade e eficiência energética.

6.3.3. Análise do mercado de fornecedores tradicionais de equipamentos RAN

Diversos países têm adotado políticas para retirar a dependência de equipamentos chineses das redes de prestadoras de telecomunicações. O Reino Unido estabeleceu a meta de ter 35% de suas redes de telecomunicações operando com equipamento *OpenRAN* até 2030 e está apoiando dezenas de projetos de desenvolvimento de *hardware* e *software* para incrementar esse esforço entre produtores nacionais.

Um relatório da Mobile Experts[60] trouxe a configuração global do *market share* dos fornecedores de rede apresentada na Figura 28 - *Market share* de redes de acesso:

[60] https://aglmediagroup.com/ericsson-tops-ran-market-mobile-experts/

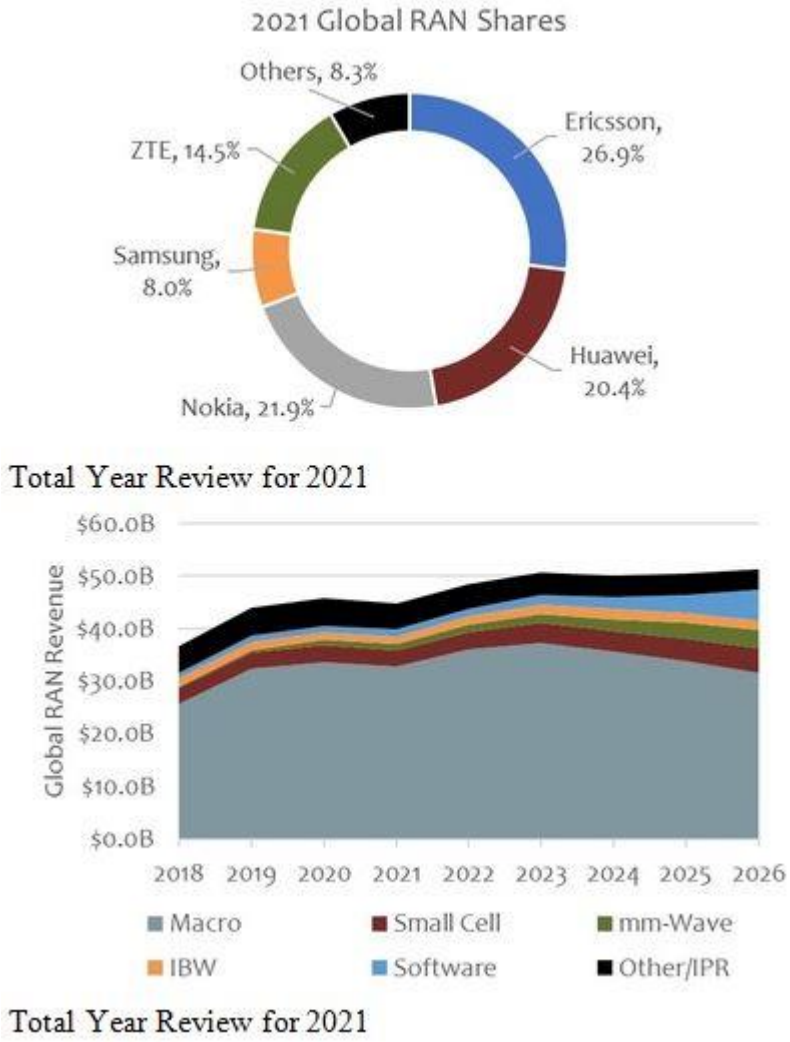

Figura 28 - *Market share* de redes de acesso

No Brasil, em 2022, verifica-se nos sistemas da Anatel que a rede brasileira é composta basicamente por três fornecedores, quais sejam, Nokia, Ericsson e Huawei, conforme Figura 29 - *Market share* de redes de acesso no Brasil:

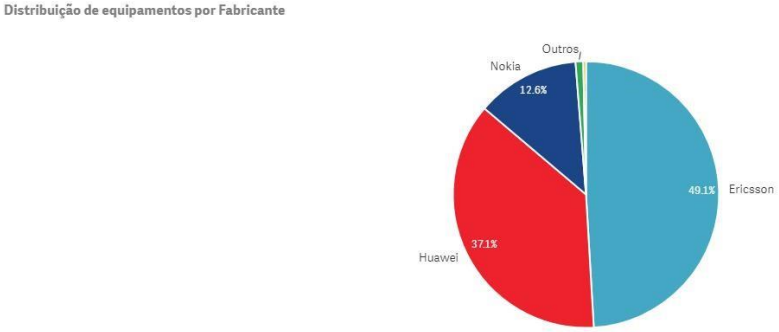

Figura 29 - *Market share* de redes de acesso no Brasil

Segundo o Mobile Experts, a Huawei em 2020 ocupava o primeiro lugar e em 2021 passou a ocupar o terceiro lugar, que seria decorrente da incapacidade da empresa em produzir estações base duplex de divisão de tempo (TDD) de alta capacidade. Outro fator atribuído pelo relatório da Mobile Experts, as sanções do governo dos EUA teriam contribuído para a queda de posição.

Provavelmente, parte significativa do entusiasmo de fabricantes em desenvolver produtos com RAN aberta decorre tanto de incentivos políticos e econômicos já explanados neste relatório, bem como no Memorando de Entendimento assinado por grandes operadoras europeias, dentre elas Deutsche Telekom AG, Orange SA, Telefónica SA, TIM e Vodafone Group Plc, para adotar *OpenRAN* como a tecnologia de escolha para futuras redes móveis, no qual divulgam orientações técnicas para auxiliar os fabricantes de equipamentos a criar *software* e *hardware* interoperáveis, posteriormente com requisitos de inteligência e automação. O objetivo é criar um ecossistema *OpenRAN* competitivo que promova abertura e flexibilidade.

Verifica-se então que um dos principais objetivos da topologia *OpenRAN* é justamente buscar ampliar a quantidade de fornecedores no mercado de equipamentos de redes móveis. Verifica-se que novos fornecedores têm surgido, principalmente em decorrência da virtualização de redes de acesso. Novos elementos de rede aberta e virtualizada tem trazido novos competidores como Altiostar, Mavenir, Parallell, bem como empresas como DELL, Sansung, NEC, IBM, HPE, Lenovo, Amazon, AWS. Portanto, empresas de *software* e provedores de conteúdo estão sendo cada dia mais incorporados nas redes de telecomunicações. Deve-se ressaltar que os provedores de nuvem inicialmente procuraram oferecer ambientes virtuais baseados em nuvem às MNOs para hospedar e executar aplicativos internos e, eventualmente, soluções externas definidas por *software*.

Um dos gargalos atuais de equipamentos para telecomunicações está em *chipsets* que possam operar em diversos tipos de dispositivos, de modo que os principais fornecedores estão engajados na proposta, como Intel, Qualcomm, Nvidia, Marvell e Xilinx.

Deste modo, a topologia *OpenRAN* visa trazer novos fornecedores ao mercado de telecomunicações, bem como se espera que os fornecedores atualmente dominantes mudem seus modelos de negócios de um *hardware* proprietário para uma abordagem mais centrada em *software*, introduzindo novos negócios e riscos competitivos durante a transição.

6.4. Subgrupo 3 – Aspectos Regulatórios

Conforme discorrido ao longo deste relatório, existem diversos aspectos regulatórios relativos à arquitetura *OpenRAN* que devem ser considerados pela Anatel. Em primeiro lugar, destaca-se a regulação já estabelecida e que guarda correlação com o tema:

a) Portaria nº 1.924/SEI-MCOM, de 29 de janeiro de 2021: Estabelece diretrizes para os certames licitatórios das faixas de radiofrequências de 700 MHz, 2,3 GHz, 3,5 GHz e 26 GHz e define critérios para a proteção dos usuários que recebem sinais

de TV aberta e gratuita por meio de antenas parabólicas na Banda C satelital, adjacente à faixa de 3,5 GHz.

> Art. 1º Estabelecer diretrizes para os certames licitatórios das faixas de radiofrequências de 700 MHz, 2,3 GHz, 3,5 GHz e 26 GHz e definir os critérios para a proteção dos usuários que recebem sinais de TV aberta e gratuita por meio de antenas parabólicas na Banda C satelital, adjacente à faixa de 3,5 GHz.
>
> Parágrafo único. Caberá à Agência Nacional de Telecomunicações - Anatel estabelecer as subfaixas a serem licitadas.
>
> Art. 2º Nas licitações de espectro de que trata o art. 1º, a Anatel deverá considerar:
>
> (...)
>
> X - incentivo à utilização de rede de acesso aberta de modo a promover interoperabilidade entre os equipamentos de diversos fornecedores.

b) Edital nº 1/2021 - Licitação nº 1/2021-SOR/SPR/CD-ANATEL – Radiofrequências nas faixas de 700 MHz, 2,3 GHz, 3,5 GHz E 26 GHz:

> Cláusula 15.2. Na contratação de serviços e na aquisição de equipamentos e materiais vinculados ao serviço objeto deste Termo, a AUTORIZADA se obriga a considerar oferta de fornecedores independentes, inclusive os nacionais, e basear suas decisões, com respeito às diversas ofertas apresentadas, no cumprimento de critérios objetivos de preço, condições de entrega e especificações técnicas estabelecidas na regulamentação pertinente.
>
> Cláusula 15.2.1. Nos casos em que haja equivalência entre ofertas, a autorizada se obriga a utilizar, como critério de desempate, a preferência a serviços oferecidos por empresas situadas no País, equipamentos, programas de computador (software) e materiais produzidos no País, e, entre eles, àqueles com tecnologia nacional. A equivalência referida neste item será apurada quando, cumulativamente:
>
> o preço nacional for menor ou igual ao preço do importado, posto no território nacional, incluídos os tributos incidentes;
>
> o prazo de entrega for compatível com as necessidades do serviço; e
>
> sejam satisfeitas as especificações técnicas estabelecidas na regulamentação pertinente e possuam certificação expedida ou aceita pela ANATEL, quando aplicável.
>
> Cláusula 15.2.2. Compreendem-se como serviços aqueles relacionados com a pesquisa e desenvolvimento, planejamento, projeto, implantação

> e instalação física, operação, manutenção, bem como a aquisição de programas de computador (software), supervisão e testes de avaliação de sistemas de telecomunicações.

A seguir, discorre-se a respeito dos aspectos regulatórios concernentes a cada um dos demais macro-eixos considerados neste relatório: Tecnológico (subdividido em Interoperabilidade e Segurança) e Econômico.

6.4.1. Macro-eixo Tecnológico - Interoperabilidade

Historicamente, a Anatel tem regulamentado a interconexão entre redes de telecomunicações, em obediência ao determinado pela Lei Geral de Telecomunicações, nos artigos 146 a 150:

> Art. 146. As redes serão organizadas como vias integradas de livre circulação, nos termos seguintes:
>
> I - é obrigatória a interconexão entre as redes, na forma da regulamentação;
>
> II - deverá ser assegurada a operação integrada das redes, em âmbito nacional e internacional;
>
> III - o direito de propriedade sobre as redes é condicionado pelo dever de cumprimento de sua função social.
>
> Parágrafo único. Interconexão é a ligação entre redes de telecomunicações funcionalmente compatíveis, de modo que os usuários de serviços de uma das redes possam comunicar-se com usuários de serviços de outra ou acessar serviços nela disponíveis.
>
> Art. 147. É obrigatória a interconexão às redes de telecomunicações a que se refere o art. 145 desta Lei, solicitada por prestadora de serviço no regime privado, nos termos da regulamentação.
>
> Art. 148. É livre a interconexão entre redes de suporte à prestação de serviços de telecomunicações no regime privado, observada a regulamentação.
>
> Art. 149. A regulamentação estabelecerá as hipóteses e condições de interconexão a redes internacionais.
>
> Art. 150. A implantação, o funcionamento e a interconexão das redes obedecerão à regulamentação editada pela Agência, assegurando a compatibilidade das redes das diferentes prestadoras, visando à sua harmonização em âmbito nacional e internacional.

A respeito desse tema, destaca-se a Resolução nº 693, de 17 de julho de 2018, que "aprova o Regulamento Geral de Interconexão - RGI e altera o Regulamento dos Serviços de Telecomunicações, o Regimento Interno da Anatel e os Regulamentos de

Remuneração pelo uso de redes do Serviço Telefônico Fixo Comutado e do Serviço Móvel Pessoal".

Em suma, a regulação da Anatel sempre esteve focada na interconexão entre redes de telecomunicações, e operação dessas redes de forma integrada.

No entanto, com a evolução das redes de telecomunicações, e visando cumprir com o objetivo de fomentar o desenvolvimento do ecossistema *OpenRAN* no Brasil, de forma a promover os diversos benefícios detalhados ao longo deste Relatório, o desafio regulatório se estendeu para dentro das redes de telecomunicações, na medida em que se vislumbrou possível necessidade de regular a interoperabilidade entre seus elementos internos que compõem essa rede.

Atualmente, a regulação de equipamentos de telecomunicações basicamente consiste no respectivo processo de certificação e homologação desses equipamentos, focada nos aspectos de: i) proteção e segurança dos usuários dos produtos para telecomunicações, ii) atendimento aos requisitos de segurança, de compatibilidade eletromagnética, de proteção ao espectro radioelétrico e de não agressão ao meio ambiente, iii) uso eficiente e racional do espectro radioelétrico, e iv) compatibilidade, operação integrada e interconexão entre as redes.

No processo de certificação e homologação, a Anatel entende não ser necessária a avaliação da interoperabilidade dos protocolos de comunicação utilizados nas interfaces internas entre os elementos de uma rede de telecomunicações quando tais protocolos são padronizados pelos fabricantes no âmbito dos respectivos fóruns internacionais: 3GPP, IEEE, ETSI, O-RAN *Alliance*, *Telecom Infra Project* (TIP), etc., conforme já detalhado neste Relatório.

Portanto, caso a Anatel decidisse por estabelecer requisitos de certificação de forma a garantir a aderência dos equipamentos aos protocolos de comunicação padronizados pelos fóruns internacionais em referência, isso seria uma mudança de paradigma de grande impacto interno, na medida que iria exigir a elaboração de todo um arcabouço regulatório de requisitos específicos para essa finalidade.

Também vale destacar que os próprios laboratórios e OCDs que compõem o sistema nacional de certificação não estariam preparados para efetuar os ensaios de tais requisitos, o que demandaria também um relevante processo de negociação, de forma a viabilizar essa mudança de paradigma.

Em complemento, é importante destacar que essa mudança de paradigma iria demandar mais tempo para conclusão dos processos de certificação e homologação de equipamentos, além de encarecer os respectivos custos.

Como já foi destacado neste relatório, o desenvolvimento do ecossistema *OpenRAN* em âmbito mundial ainda está nos seus estágios iniciais, com poucas operações comerciais relevantes, e ainda há muita discussão nos respectivos fóruns internacionais a respeito da padronização das interfaces vinculadas à *OpenRAN*.

Portanto, no atual contexto, entende-se que o mais prudente seria a Anatel seguir acompanhando a evolução deste ecossistema, sem impor nesse momento requisitos

específicos de certificação de interoperabilidade entre elementos internos de redes de telecomunicações.

No entanto, desde já cabe destacar que, na medida que o conceito básico de *OpenRAN* é permitir que uma determinada empresa que queira implementar uma operação de rede de telecomunicações baseada em tecnologia 5G possa desenvolver sua rede com elementos de variados fornecedores de equipamentos, é importante que essa empresa receba o devido suporte tecnológico, para que todos esses elementos sejam efetivamente interoperáveis, visando garantir o funcionamento da rede 5G com todos os recursos desejados pela empresa, e com desempenho adequado de *throughput*, latência, cobertura, etc.

E caso se constate algum problema de interoperabilidade, a empresa não seja vítima de uma indefinição sobre a responsabilidade dos diversos fornecedores, que pode até acarretar disputas judiciais que, pelo seu caráter eminentemente técnico, podem demandar tempo para resolução.

Neste escopo, a Anatel continuará acompanhando as regras de padronização internacional a fim de verificar se eventuais problemas relativos à interoperabilidade serão endereçados por tais padrões. Caso sejam identificados problemas, poderia ser criado um fórum específico de fornecedores de equipamentos para o ecossistema *OpenRAN*, que teria o condão de acompanhar as implementações dessas redes no país, avaliar eventuais dificuldades e/ou restrições, e atuar como mediadora entre as partes conflitantes, caso necessário.

6.4.2. Macro-eixo Tecnológico - Segurança

A respeito desse tema, a Anatel emitiu a Resolução nº 740 de 21 de dezembro de 2020 – Aprova o Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações.

Este Regulamento está focado em regular a atuação dos prestadores de serviços de telecomunicações, de forma a mitigar riscos de danos por ataques cibernéticos às suas respectivas redes.

Da mesma forma que no processo de certificação e homologação a Anatel não avalia a interoperabilidade dos protocolos de comunicação utilizados nas interfaces internas entre os elementos de uma rede de telecomunicações, presentemente, também não é avaliada a segurança de tais protocolos, ou o grau de robustez dos equipamentos de telecomunicações para mitigar ataques cibernéticos.

Compreende-se que a avaliação da segurança cibernética em produtos difere da avaliação da conformidade já realizada pela Anatel por meio do processo de certificação dos produtos. O processo de certificação atualmente aplicado pela Agência realiza avaliações de parâmetros determinísticos, cujo comportamento não se altera no decorrer do tempo, tais como: máxima potência de transmissão, largura de banda e emissões espúrias de radiofrequência. Para todos esses parâmetros são conhecidos os limites máximo e mínimo para atendimento dos requisitos e quais os procedimentos de ensaios padronizados aplicáveis para sua verificação. Já a avaliação de segurança

cibernética é realizada sobre parâmetros dinâmicos: a cada dia são descobertas novas vulnerabilidades em produtos ou agentes mal-intencionados desenvolvem novas técnicas para explorar funcionalidades de equipamentos que, até aquele momento, eram consideradas seguras.

A Anatel tem atuado de forma a acompanhar o cenário normativo internacional a fim de determinar qual a maneira adequada para avaliar a segurança cibernética de produtos. Em janeiro de 2021 a Agência publicou o Ato nº 77, de 05 de janeiro de 2021, que aprovou os Requisitos de Segurança Cibernética para Equipamentos para Telecomunicações. Este documento apresenta um conjunto de recomendações de segurança que fabricantes e fornecedores de equipamentos devem adotar no ciclo de vida de seus produtos, desde a concepção, aplicando-se o conceito de *security-by-design*, até a fase de vendas e suporte ao consumidor, adotando estratégias de identificação e correção de vulnerabilidades em produtos já disponíveis no mercado.

O conjunto de requisitos aprovados pelo Ato nº 77, de 05 de janeiro de 2021, tem caráter recomendatório, contudo, a Anatel pode definir que determinados requisitos de segurança do documento sejam mandatórios no processo de certificação de determinados produtos, a depender das características dos equipamentos e de vulnerabilidades reconhecidamente tidas como comuns a estes dispositivos. Um exemplo dessa forma de atuação é a Consulta Pública nº 65 de 2022, que propôs um conjunto de verificações mandatórias para a certificação de CPEs (*Customer Premises Equipment* ou *Customer Provided Equipment*, Equipamento nas Instalações do Cliente) que, reconhecidamente, apresentam a vulnerabilidade de senha padrão (senhas fornecidas de fábrica iguais entre todos os equipamentos produzidos ou baseadas no seu endereço MAC).

Apesar da avaliação da segurança cibernética ser uma quebra de paradigmas no processo de avaliação da conformidade de produtos, compreende-se que, para determinados tipos destes produtos, será necessário determinar que algumas avaliações de segurança sejam realizadas em seu processo de certificação para garantir um perfil mínimo de segurança.

Em uma primeira avaliação, compreende-se que a padronização em desenvolvimento para os equipamentos *OpenRAN* irá endereçar de forma adequada os problemas de segurança identificados nesta nova arquitetura e em seus equipamentos. Caso a Anatel identifique, no decorrer da implantação e do uso da nova tecnologia, que determinadas características ou vulnerabilidades já conhecidas devam ser endereçadas no processo de certificação dos equipamentos para *OpenRAN*, a Agência, por meio de sua Superintendência competente, poderá definir requisitos mandatórios para avaliação da segurança cibernética destes equipamentos, sempre de forma alinhada às recomendações e *frameworks* adotados internacionalmente, a fim de não criar barreiras técnicas para a introdução dos produtos no país.

Também vale destacar que os laboratórios e OCDs que compõem o sistema nacional de certificação atualmente não estão totalmente preparados para efetuar os testes de tais requisitos. Contudo, muitos estão se capacitando para realizar avaliações de

segurança em produtos, inclusive para a realização de testes de mais alta complexidade, como *pen-testing* em equipamentos.

Em complemento, é importante destacar que essa mudança de paradigma no processo de certificação poderá aumentar ainda mais o tempo para conclusão dos testes executados no processo de certificação e homologação de equipamentos, além de encarecer os respectivos custos. A Agência está estudando qual a melhor forma para realização de tais avaliações, considerando as vantagens e desvantagens de uma avaliação pré-mercado (no processo de certificação do produto) ou de pós-mercado (em atividades de supervisão de mercado nas quais os produtos podem ser avaliados continuamente quanto à sua segurança, à medida que novas falhas e vulnerabilidades são identificadas).

Além disso, ressalta-se que a questão da regulamentação da segurança cibernética de sistemas de telecomunicações envolve outros órgãos e entes, tais como a Autoridade Nacional de Proteção de Dados (ANPD) e Comitê Gestor da Internet (CGI.BR). Portanto, as atribuições regulatórias da Anatel nesse tema teriam que ser devidamente equacionadas nesse contexto multidisciplinar.

Destaca-se que a Anatel já estabeleceu um Grupo Técnico específico para tratar de segurança cibernética de redes de telecomunicações – o Grupo Técnico de Segurança Cibernética e Gestão de Riscos de Infraestrutura Crítica (GT-Ciber). Portanto, é recomendável que este tema seja discutido conjuntamente com o GT-Ciber, para avaliação dos próximos passos.

6.4.3. Macro-eixo Econômico

Em termos de regulação desse macro-eixo, entende-se que estaria mais focada no fomento do ecossistema *OpenRAN*, promovendo assim o desenvolvimento de redes 5G em suas mais diversas aplicações no país, e por consequência propiciando benefícios econômicos para toda a sociedade brasileira.

Quanto a isso, é importante destacar as iniciativas já em curso no país, como o acordo de cooperação com recursos para desenvolvimento da arquitetura aberta no Brasil, assinado pelo Ministério da Ciência, Tecnologia e Inovações, conforme citado na seção 6.2 supra.

Adicionalmente, destaca-se o projeto 5GBR, que tem como objetivo desenvolver tecnologias 5G de arquitetura aberta, virtualizada e desagregada, com provas de conceito para o mercado de redes privativas e ISPs. O projeto conta com recursos do Funttel, portanto é vinculado ao Ministério das Comunicações, conforme citado no item 5.3 supra.

No entanto, para fomentar o desenvolvimento do ecossistema *OpenRAN* no país, é muito importante ampliar essas iniciativas, aproximando a academia e a indústria nacional de *hardware* e *software*, visando não só o desenvolvimento de produtos e serviços, mas também a promoção de capacitação maciça de pessoas para impulsionar esse desenvolvimento tecnológico no país, ampliando o conhecimento nacional sobre o assunto, bem como geração de empregos.

Uma forma de ampliar essas iniciativas seria a divulgação de orientações aos interessados em obterem financiamento para projetos vinculados ao ecossistema *OpenRAN* para conseguirem acessar os recursos do Funttel, bem como otimizar os procedimentos exigidos para liberação desses recursos, além do acompanhamento dos resultados obtidos com tais projetos e respectiva disseminação para o setor de telecomunicações, promovendo assim um ciclo realimentado de desenvolvimento do ecossistema *OpenRAN* no Brasil.

Outra iniciativa relevante nesse macro-eixo seria promover uma redução da carga tributária de produtos e serviços vinculados ao ecossistema *OpenRAN*, visando o desenvolvimento de redes 5G que tem o condão de impulsionar o crescimento da economia nacional nos mais variados setores – indústria 4.0, agropecuário, transportes, educação, saúde etc.

7. ETAPA 3 – PROPOSIÇÃO

Com as informações advindas dos estudos, reuniões e comentários obtidos durante as primeiras duas etapas do GT *OpenRAN*, faz-se necessário consolidá-las e produzir uma síntese dos diferentes eixos temáticos. Avaliar o caminho a seguir e identificar cenários de uso e de implementação das tecnologias e frameworks *OpenRAN* são importantes instrumentos para identificar potenciais desafios e adequações tecnológicas, regulatórias e configurações de valor no âmbito da indústria e do mercado de Telecomunicações.

A partir da reflexão e compreensão das possibilidades e dos modelos de implementação que emergem do arcabouço tecnológico da topologia *OpenRAN* no cenário brasileiro, hipóteses foram formuladas e novas realidades puderam ser projetadas a partir da transformação tecnológica desencadeada.

Pode-se, então, identificar os potenciais fatores habilitadores para impulsionar *OpenRAN* no Brasil, primando pelos domínios estratégicos e operacionais e pelas potencialidades e condicionamentos – oportunidades e desafios que lhe são inerentes, em cada linha temática proposta.

7.1. *Sandbox* regulatório

A Lei Complementar nº 182, de 1º de junho de 2021, institui o marco legal das *startups* e do empreendedorismo inovador e dá outras providências. Entre outras determinações, a LC nº 182 apresenta o conceito de ambiente regulatório experimental, também chamado *sandbox* regulatório, no inciso II do art. 2º:

> Ambiente regulatório experimental (*sandbox* regulatório): conjunto de condições especiais simplificadas para que as pessoas jurídicas participantes possam receber autorização temporária dos órgãos ou das entidades com competência de regulamentação setorial para desenvolver modelos de negócios inovadores e testar técnicas e tecnologias experimentais, mediante o cumprimento de critérios e de

> limites previamente estabelecidos pelo órgão ou entidade reguladora e por meio de procedimento facilitado.

Assim, a legislação brasileira procura estimular a inovação tecnológica permitindo a criação de ambientes de testes para que se desenvolvam com segurança e incentivo modelos de negócios e tecnologias inovadores. Em linhas gerais, é um ambiente experimental constituído com condições especiais, limitadas e exclusivas com o intuito de não permitir barreiras à inovação, com o objetivo de reduzir custos e facilitar o desenvolvimento de tecnologias disruptivas.

A LC nº 182, em seu art. 11, estabelece que órgãos e entidades da administração pública com competência de regulamentação setorial poderão, individualmente ou em colaboração, no âmbito de programas de ambiente regulatório experimental, afastar a incidência de normas sob sua competência em relação à entidade regulada ou aos grupos de entidades reguladas. Logo, cumpre ao ente público competente estabelecer as regras específicas de um possível *sandbox* regulatório sob sua esfera de atuação.

Internacionalmente, o tema *sandbox* foi, inclusive, mote da *Global Conference on Governance Innovation: Towards agile regulatory frameworks in the fourth industrial revolution*, evento da Organização para a Cooperação e Desenvolvimento Econômico (OCDE). Conforme *Going Digital Steering Group Meeting* ocorrido em 19 de outubro de 2018, com participação de delegado da Anatel, foi identificada oportunidade de implementar o conceito de *sandboxes* regulatórios para potencializar a inovação no ambiente regulatório do setor de telecomunicações. Das notas deste encontro, presentes no processo SEI nº 53500.051610/2019-15:

> *Policymakers are increasingly experimenting to promote flexibility and innovation. One approach to develop mechanisms that promote the flexible application or enforcement of policies is the use of regulatory 'sandboxes', which may be particularly useful for certain kinds of digitally-enabled innovation.*

Segundo a OCDE, *sandbox* regulatório se refere a uma forma limitada de flexibilidade regulatória para as empresas que permita testar novos modelos de negócios e tenha carga regulatória reduzida. Os *sandboxes* regulatórios geralmente incluem mecanismos destinados a garantir objetivos regulatórios abrangentes, incluindo a proteção do consumidor.

Na Europa há algumas iniciativas[61]. Este *benchmark* mostra que os *sandboxes* regulatórios nas áreas de proteção de dados, tecnologias relacionadas a dados (como inteligência artificial, carros conectados e identidade digital) e telecomunicações ainda são incipientes na Europa. Apenas França, Alemanha e Reino Unido criaram *sandboxes* regulatórios gerenciadas por diferentes autoridades.

[61] https://www.cullen-international.com/client/site/documents/CTECEU20220018

No âmbito da União Europeia, o projeto de Lei de Inteligência Artificial[62] prevê o estabelecimento de *sandboxes* regulatórios de IA pelas autoridades nacionais competentes e pela Autoridade Europeia para a Proteção de Dados para facilitar o teste e a validação de sistemas inovadores de IA antes da sua colocação no mercado.

A ARCEP, reguladora francesa do setor, tem *sandbox* regulatório com foco em projetos inovadores que se baseiam na utilização de radiofrequências e recursos de numeração. O quadro experimental permite que as empresas fiquem isentas, total ou parcialmente, das obrigações relacionadas com a utilização de frequências e recursos de numeração, por exemplo, por um período máximo de dois anos. As isenções são decididas caso a caso.

Na Alemanha, O Ministério Federal de Assuntos Econômicos e Energia (BMWK) publicou em dezembro de 2018 uma estratégia sobre *sandboxes* regulatórios. Com base na estratégia, a BMWK apresentou em 2021 uma proposta de lei federal de experimentação que forneceria uma estrutura com condições uniformes e favoráveis à inovação para *sandboxes* regulatórios. 27 *sandboxes* regulatórios existentes ou planejadas nas esferas federal e regional foram relatadas em uma pesquisa de 2019[63].

A autoridade britânica de informação, ICO, tem sob sua área de ação alguns focos para o *sandbox* no período de 2021 a2022, como compartilhamento de dados na esfera pública e produtos e serviços que usam tecnologias inovadoras, como aprimoramento de privacidade e contabilidade distribuída[64].

Outros países europeus que estão com iniciativas relacionadas a *sandboxes* regulatórios em estudo ou andamento incluem Irlanda, Espanha e Bélgica.

O regulador colombiano, *Comisión de Regulación de Comunicaciones* – CRC, foi o primeiro ente na América do Sul a instituir *sandbox* no ambiente de comunicações, também com período predefinido para inscrições, quantidade limitada de vagas e prazo de duração dos testes predeterminado. Neste caso específico, a primeira rodada de oportunidades admitiu três projetos[65] dentre 23 apresentados:

- *Internet en las zonas rurales y periurbanas a través de cobertura móvil celular 4G Open RAN*, da empresa Colombia Telecomunicaciones S.A. ESP, que visava fornecer cobertura móvel celular 4G em áreas rurais e periurbanas.
- *Herramienta SOC (Service Operation Center)*, da mesma Colombia Telecomunicaciones S.A. ESP, teve como foco a implementação de uma

62 https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf

63 https://www.bmwk.de/Redaktion/EN/Publikationen/Digitale-Welt/handbook-regulatory-sandboxes.pdf?__blob=publicationFile&v=2

64 Contabilidade distribuída é uma tecnologia que permite a realização de qualquer transação, alegadamente de forma segura e confiável, sem a necessidade de intermediários, através da Internet. A primeira iniciativa documentada foi a criptomoeda *Bitcoin*, baseada na plataforma *blockchain*.

65 https://www.crcom.gov.co/es/noticias/comunicado-prensa/conozca-proyectos-admitidos-para-experimentacion-en-sandbox-regulatorio

plataforma para a medição real da experiência dos usuários do serviço de internet móvel.

- *Contrato Convergente*, da empresa Colombia Móvil S.A. ESP, que visa simplificar o processo de contratação de serviços fixos e móveis pós-pagos para cidadãos, através de um contrato unificado para a prestação dos referidos serviços.

Destes, o projeto *Internet en las zonas rurales y periurbanas a través de cobertura móvil celular 4G Open RAN* foi abandonado pela empresa[66]. Os demais continuam em andamento.

Esta experiência da CRC é uma das referências que foram consideradas no estudo realizado pela Anatel para a criação da regulamentação para ambiente regulatório experimental. Este estudo faz parte de uma iniciativa mais ampla, que visa atualizar o Regulamento sobre Uso Temporário de Radiofrequências (RUTE), aprovado pela Resolução nº 635, de 9 de maio de 2014, a fim de contemplar inovações oriundas da atualização do Serviço Especial para Fins Científicos e Experimentais (SEFICE) e da introdução do conceito *sandbox* regulatório, este inserido nos Projetos da Simplificação da Regulamentação de Serviços de Telecomunicações, conforme processo SEI nº 53500.059638/2017-39. Atualmente há uma proposta de resolução em avaliação pela Anatel que já superou a etapa de consulta pública.

Nacionalmente, no momento do desenvolvimento deste relatório, três iniciativas de *sandboxes* regulatórios estão em andamento no país, do Banco Central do Brasil[67], da Superintendência de Seguros Privados[68] e da Comissão de Valores Mobiliários[69]. Estas três iniciativas têm em comum alguns parâmetros, como período predefinido para inscrições, quantidade limitada de vagas e prazo de duração dos testes predeterminado.

Assim, vale salientar uma diferença estrutural de um *sandbox* regulatório no ambiente de telecomunicações com relação às iniciativas já em andamento no Brasil, do BCB, CVM e Susep: o uso de radiofrequências. Nos mercados bancário, de valores mobiliários e de seguros, a delimitação territorial não necessariamente será causa de prejuízos aos consumidores ou à competição. Já um ambiente regulatório experimental que faça uso de radiofrequências dependerá, dentre outros parâmetros, da definição de um polígono que impeça a emissão de radiofrequências em seu exterior.

Neste sentido, a autorização para uso temporário de radiofrequências precisará se adequar às características e à finalidade do *sandbox* regulatório, em especial quanto à duração da autorização e à possibilidade de sua utilização com caráter comercial. Estes estudos fazem parte dos trabalhos nos Projetos da Simplificação da Regulamentação de Serviços de Telecomunicações da Anatel.

[66] https://www.crcom.gov.co/sites/default/files/normatividad/00006529.pdf
[67] https://www.bcb.gov.br/estabilidadefinanceira/sandbox
[68] https://www.sandbox.susep.gov.br/
[69] https://conteudo.cvm.gov.br/legislacao/sandbox_regulatorio.html

Voltando à experiência colombiana, a alegação da operadora Coltel ao desistir do *sandbox* regulatório para estudar *OpenRAN* foi:

> *Teniendo en cuenta que actualmente se tiene un nivel alto de incertidumbre en la adquisición de espectro radioeléctrico en el País, debido al alto valor que el Ministerio de las TIC ha definido en el proceso de renovación de la banda de 1900 MHz, por lo cual, la compañía ha decidido suspender los recursos asignados al proyecto en mención hasta tanto se pueda tener un nivel de negociación del espectro que permita a Colombia Telecomunicaciones S.A. ESP BIC hacer usos del espectro a un precio razonable.*

Na explanação constante da *Resolución nº 6529 de 2022*, que formaliza a desistência da Coltel em operar o projeto, não fica claro se a aquisição da faixa de 1900 MHz citada tinha por finalidade o uso no *sandbox* regulatório, tornando esse projeto mais caro do que o previsto, ou para as operações regulares da empresa, que precisou fazer um rearranjo em suas finanças para explorar essa faixa e precisou renunciar ao *sandbox* regulatório para não prejudicar sua operação regular.

Porém, independentemente de qual seja o motivo para a renúncia, resta clara a importância de que as autorizações para o *sandbox* regulatório e de uso temporário do espectro, caso esta seja necessária para aquela, sejam analisadas em conjunto e possuam regulamentação compatível, pelo qual a Anatel tem estudado o tema com o maior detalhamento possível.

Outro ponto que está percorrendo as experiências realizadas ou em andamento de *sandboxes* regulatórios que foram estudadas, tanto no âmbito nacional quanto internacional, é a existência de períodos específicos para início dos projetos, com abertura formal de intervalo de tempo para inscrições. Neste sentido, seria interessante permitir a solicitação de autorização de *sandbox* regulatório e de uso de radiofrequências associadas a qualquer momento, nos mesmos moldes de autorizações emitidas pela Anatel em geral, a fim de permitir que iniciativas disruptivas possam alavancar o desenvolvimento tecnológico no setor de telecomunicações, evitando a criação de barreiras desnecessárias ao mercado.

7.2. Localização de *data centers*

No mercado de telecomunicações empresas têm se valido da terceirização de *data centers*, uma vez que a estrutura depende de equipamentos modernos e atualizados e de uma conexão de internet de ótima qualidade para garantir o desempenho esperado, além de uma equipe de profissionais especializados, o que, muitas vezes, onera a folha de pagamento. Por se tratar de prestação de serviço baseado em nuvem, abre-se a possibilidade de contratação de prestadores em qualquer lugar do mundo. Não obstante essa alternativa, há algumas vantagens no uso de *data centers* locais[70]:

[70] https://odatacolocation.com/blog/data-center-no-brasil-ou-no-exterior/

- Redução de custos: o fornecedor local permite eliminação de custos relevantes em *hardware* e com a manutenção das instalações, migração de CAPEX para OPEX, já que a alocação dos equipamentos em um *data center* terceirizado é contratada como serviço e não há custos relacionados a transações internacionais, ou seja, há isenção de IOF (imposto sobre operações financeiras), pagamento em moeda local e independência da variação cambial.

- Superação de desafios operacionais: um provedor de *data center* local pode proporcionar agilidade à operação por conta da latência reduzida. Isso porque, por estar mais próximo das instalações da empresa cliente, a conexão de internet tem uma entrega mais rápida e estável.

- Velocidade do tempo de resposta: um fornecedor local pode assegurar uma resposta mais ágil às necessidades do cliente, especialmente em situações de crise, nas quais seja necessário colocar em prática a recuperação de desastres.

7.3. Perfis de interoperabilidade

De uma maneira ampla, as entidades que se propõem a padronizar a topologia *OpenRAN* têm um modelo certificatório baseado em três níveis. O primeiro procura garantir a conformidade de cada módulo individualmente. O segundo visa certificar a interoperabilidade entre módulos. O terceiro, a interoperabilidade da solução completa, chamada *end-to-end* ou E2E. Vale ressaltar que este modelo certificatório não substitui a avaliação baseada nos conceitos do 3GPP, nos quais a Anatel se baseia para emitir seus requisitos técnicos de avaliação da conformidade de transceptores para estações rádio base, por exemplo.

Vale ressaltar que associações como *Small Cell Forum* e O-RAN *Alliance* têm trabalhado na definição de *blueprints*, conjuntos de entradas usados para descrever uma implantação específica de sistema ou solução baseados em *OpenRAN*, que pode incluir a especificação da implantação de sistemas (por exemplo, arquitetura, métricas de desempenho) como no e de subsistemas e as interfaces entre os subsistemas especificados. Isso permitiria a definição e documentação da metodologia e de casos de teste. A definição de *blueprints* ajuda a restringir a quantidade de perfis de interoperabilidade a serem padronizados.

Na definição da O-RAN *Alliance*[71], um perfil de interoperabilidade é *uma seleção específica de parâmetros, recursos opcionais, valores padrão e faixas de atributos e mecanismos configuráveis de especificações de interface O-RAN que devem ser suportados e usados para garantir a interoperabilidade entre implementações de diferentes fornecedores*.

Interfaces padronizadas são a característica da topologia *OpenRAN* que permite a interoperabilidade entre módulos de diferentes fornecedores. Para garantir a

[71] O-RAN.TIFG.Cert-Badge.0-v04.00 *O-RAN ALLIANCE Test and Integration Focus Group Certification and Badging Processes and Procedures*.

interoperabilidade, associações como O-RAN *Alliance* e TIP se propõem a fazer ensaios de certificação e emitir *badges* que comprovam a compatibilidade entre elementos e unidades de diferentes fabricantes. As certificações O-RAN procuram garantir que um equipamento ou função está em conformidade com as especificações O-RAN e os *badges* O-RAN buscam confirmar a interoperabilidade ou a funcionalidade de ponta a ponta de uma solução O-RAN. Os certificados e *badges* O-RAN Alliance são emitidos pelos *Open Testing and Integration Centers*, ou OTICs. Já os *badges* e *ribbons* TIP garantem, em diferentes níveis, a conformidade e a compatibilidade de soluções *OpenRAN*. Os *badges* e *ribbons* TIP são emitidos pelos *Community Labs*.

Porém, enquanto a O-RAN *Alliance* se propõe a emitir normas de padronização, incluindo requisitos de interoperabilidade, o TIP entende que a normatização deve ficar sob a tutela de órgãos estabelecidos para a emissão de normas, inclusive a própria O-RAN *Alliance*. Neste sentido, o TIP pode emitir sua certificação baseada também na própria normatização da O-RAN *Alliance*.

Focando exclusivamente em interoperabilidade, um aspecto relevante é a padronização das interfaces. Em uma rede aberta, há interfaces oriundas das definições do 3GPP, tais como X2/Xn e F1, e outras exclusivas para a topologia aberta. Neste sentido, cumpre ressaltar que, dependendo da *split* adotada, a padronização da interface utilizada se altera. Como visto na subseção Topologias e *splits*, o 3GPP recomenda a *split* 2 para aplicações centralizadas, como acesso sem fio fixo (FWA), onde a coordenação do local da célula não é necessária e os requisitos de latência e largura de banda na rede de transporte são menos exigentes, a opção 6 está sendo promovida pelo *Small Cell Forum* (SCF), como a divisão ideal para implantações de baixo custo e baixa capacidade, cujas especificações são conhecidas como nFAPI e, por fim, a O-RAN *Alliance* oferece suporte à opção 7.2 para redes com requisitos de alta capacidade e confiabilidade.

Em relação às especificações da O-RAN *Alliance*, é possível verificar que algumas interfaces, mas não todas, estão com a padronização definida, conforme reunião (SEI nº 8801345) ocorrida em 13/07/2022 com representante de indústria associada à aliança:

- F1 - especificação incompleta
- W1 - especificação incompleta
- E1 - especificação incompleta
- X2 - especificação parcialmente disponível
- Xn - especificação incompleta
- FH - especificação da eCPRI na *split* 7-2x disponível
- E2 - especificação disponível
- A1 - especificação disponível

- O1 - especificação disponível
- O2 - especificação incompleta

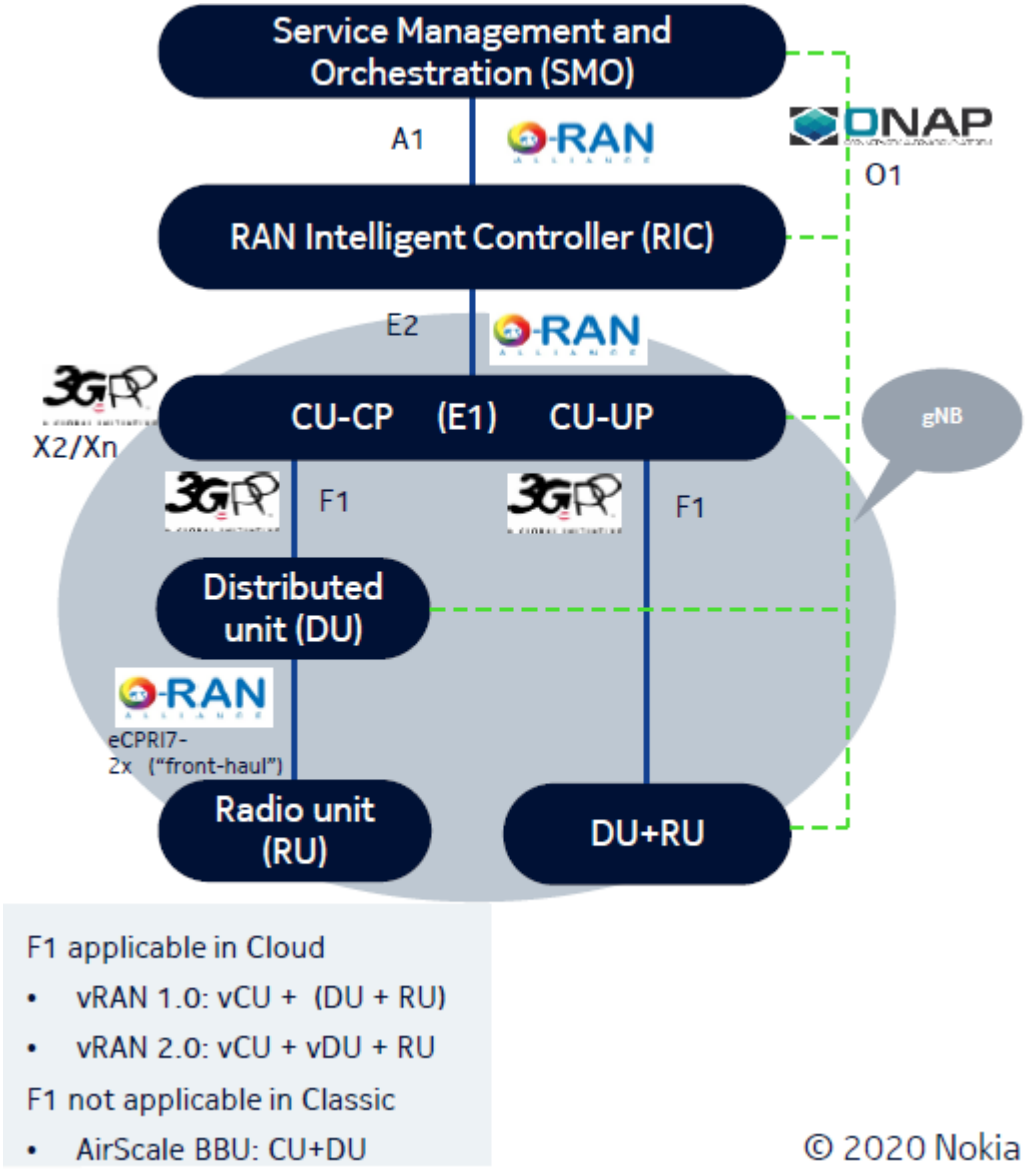

Figura 30 - Interfaces *OpenRAN*

Porém, na mesma reunião foi informado que as especificações emitidas até este momento são suficientes para garantir a interoperabilidade entre a RU e a DU. Isso significa que uma RU excitada por uma DU através de uma interface *fronthaul* que siga as especificações da O-RAN *Alliance* conseguirá emitir uma portadora compatível com a máscara de emissão prevista na regulamentação vigente, assim como ativar corretamente os planos de controle, usuário, sincronismo e gerenciamento (*C/U/S/M-plane*s), mas não necessariamente que conseguirá prestar o serviço esperado. A compatibilidade de facilidades e verificação de performance destas facilidades não é abarcado pelas especificações da aliança, de forma que o operador da rede deverá se responsabilizar por esta etapa da certificação.

Neste sentido, verifica-se que a abordagem de certificação da O-RAN *Alliance* possui pontos de convergência com o processo de avaliação da conformidade da Anatel, no qual requisitos mínimos são ensaiados para garantir um padrão básico para o uso do produto de telecomunicações. Assim, reforça-se a posição de que a Anatel não necessitaria criar requisitos técnicos para avaliação da conformidade específicos para produtos *OpenRAN*, uma vez que já existem diferentes organizações setoriais trabalhando na definição de requisitos de conformidade de produtos, de interoperabilidade, de certificação E2E e mesmo de *blueprints*.

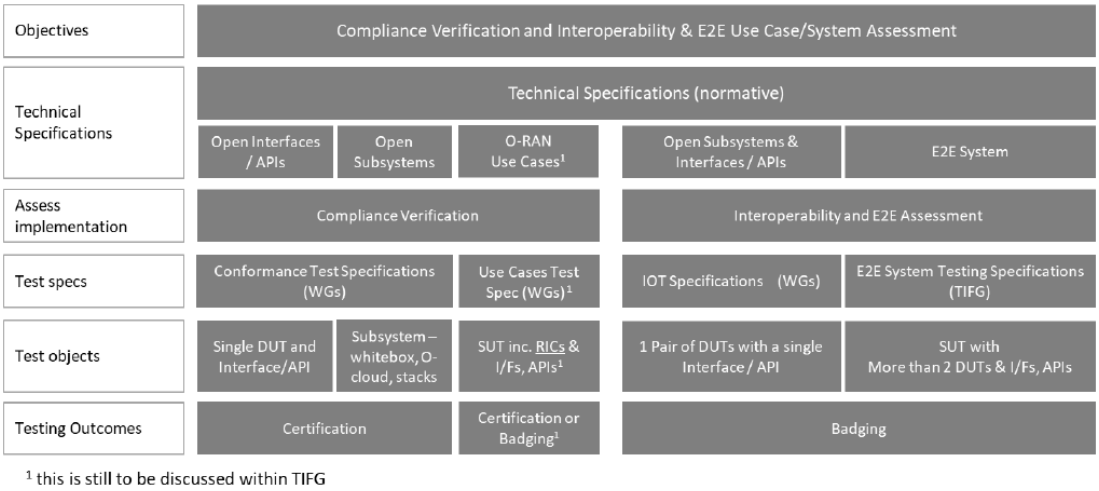

Figura 31 - Conceito de certificação e *badging* da O-RAN *Alliance*

7.4. Requisitos de cibersegurança

A introdução de novos componentes, interfaces abertas, desagregação e integração de lógica de controle personalizada e possivelmente orientada a podem tornar as redes celulares de próxima geração mais eficientes e flexíveis. Por outro lado, essa revolução vem com desafios de segurança que decorrem principalmente do fato de que a natureza distribuída e desagregada da topologia *OpenRAN* aumenta a superfície de ataque para usuários mal-intencionados, representando ameaças graves à rede e seus usuários.

As tecnologias e arquiteturas de rede em evolução também estão expandindo o segmento de clientes das operadoras, de consumidores a empresas e indústrias, permitindo novos mercados e mecanismos de crescimento. Mas, ao mesmo tempo, este incremento introduz complexidade e aumenta a potencial superfície de ataque e o risco apresentado pela infraestrutura de acesso de rádio.

Não obstante, novos recursos de monitoramento, inteligência e implantação em nuvem que caracterizam as redes abertas permitem melhor acompanhamento sobre o estado da rede e fornecem as ferramentas para monitorar, detectar, prevenir e neutralizar ameaças. Neste sentido, a O-RAN *Alliance* criou um subgrupo dedicado, o *Security Focus Group* (SFG) para a análise e definição de modelos de ameaças para redes abertas, bem como para a definição de medidas e políticas de segurança para os componentes da topologia *OpenRAN*.

Como visto na subseção Subgrupo 1B – Segurança, o Escritório Federal de Segurança da Informação da Alemanha (BSI) elaborou análise de risco, onde se verificou que muitos interfaces e componentes especificados em *OpenRAN* apresentam riscos de segurança médios a altos, uma vez que o atual processo de desenvolvimento das especificações *OpenRAN* não é baseado no paradigma de *security/privacy by design/default*" e os princípios de segurança multilateral (suposições mínimas de confiabilidade em relação a todas as partes envolvidas, também chamados *zero trust*) não foram levados em conta[32].

As indicações iniciais são de que a O-RAN *Alliance* aumentará o escrutínio dado ao tema da segurança no futuro. Conforme o relatório do BSI, a experiência passada mostra que a adição de medidas de segurança em um estágio tardio leva a custos muito altos ou a soluções inseguras ou – não raramente – a ambos. O desenvolvimento dos padrões 3GPP é um bom exemplo disso. A tentativa de corrigir esses erros em versões subsequentes dos padrões 3GPP tem sido cara e muitas vezes levou – principalmente pela necessidade de fornecer compatibilidade – a soluções que permaneceram inseguras.

Uma grande variedade de melhorias de segurança *OpenRAN* são sugeridas pelos autores do estudo do BSI, incluindo[72]:

- Implementar confiança zero/segurança multilateral.
- Prescrever *backup* opcional na camada de transporte.
- Usar o protocolo de criptografia de comunicações TLS em vez de SSH2.
- Restringir o impacto potencial de ataques de negação de serviço nas interfaces.
- Implementar um *design* amigável ao *firewall*.
- Exigir que linguagens de programação seguras como Rust sejam usadas para automação de xApps e rApps.
- Autenticação obrigatória do usuário para a plataforma O-Cloud de nós usando a arquitetura *OpenRAN*.

Existem outras recomendações importantes, que destacam até que ponto este estudo identifica possíveis pontos de melhoria para os padrões de segurança na topologia *OpenRAN*.

Já no âmbito da União Europeia[73], seus Estados-Membros, com o apoio da Comissão Europeia e da Agência da UE para a Cibersegurança (ENISA), desenvolveram uma abordagem focada em segurança de redes 5G. Através desta abordagem, avaliou-se em

[72] https://commsrisk.com/german-study-warns-5g-open-ran-is-not-secure-by-design/
[73] EU-wide coordinated risk assessment of 5G networks security, 9 October 2019, https://digital-strategy.ec.europa.eu/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security

conjunto os riscos relacionados com as redes 5G e foram identificadas medidas para redução dos riscos apresentadas sob a forma de uma *toolbox*[74] em janeiro de 2020. Desde que a *toolbox* foi adotada, a topologia *OpenRAN* recebeu atenção e interesse significativos[75]. Com o desenvolvimento de interfaces abertas, mas não necessariamente com padrões abertos, além de outros habilitadores para *OpenRAN* como a divisão e a desagregação de diferentes funções de rede e a cloudificação e virtualização de funções de rede, a topologia *OpenRAN* poderia contribuir para garantir a diversidade de fornecedores para MNOs individuais por meio de estratégias apropriadas de vários fornecedores para evitar ou limitar qualquer grande dependência de um único fornecedor.

Dentre outras verificações, o relatório sobre Cibersegurança em *OpenRAN* da UE procurou realizar uma análise de segurança aprofundada a fim de identificar o impacto da RAN aberta nos riscos de segurança das redes 5G já identificadas na Avaliação de risco coordenada da segurança cibernética 5G[73] e identificação e avaliação de potenciais novos riscos de segurança e potenciais oportunidades de segurança relacionadas à topologia *OpenRAN*.

Como também identificado em outros estudos e apresentado neste relatório, além de desafios e oportunidades específicos à segurança de redes abertas para além das redes de acesso via rádio tradicionais, o relatório da UE entende ser necessário implementar outras ações, tais como:

- Usar poderes regulatórios para poder examinar planos de implantação de *OpenRAN* em larga escala de MNOs e, se necessário, restringir, proibir e/ou impor requisitos ou condições específicas para o fornecimento, implantação e operação em larga escala do equipamento de rede aberta.

- Reforçar os principais controles técnicos, como autenticação e autorização, e adaptar o *design* de monitoramento a um ambiente modular onde cada componente é monitorado.

- Avaliar o perfil de risco de provedores de rede aberta, provedores de serviços externos relacionados a *OpenRAN*, provedores de serviços e infraestrutura em nuvem e integradores de sistemas, e estender os controles e restrições sobre provedores de serviços gerenciados[76] (*Managed Service Providers*, MSPs) a esses provedores.

- Garantir que o processo deve satisfazer os princípios do Acordo sobre Barreiras Técnicas ao Comércio da Organização Mundial do Comércio,

[74] Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures, 29 January 2020, https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures
[75] Cybersecurity of Open Radio Access Networks, 11 May 2022, https://ec.europa.eu/newsroom/dae/redirection/document/86603
[76] Um provedor de serviços gerenciados (MSP) é uma empresa terceirizada que gerencia remotamente a infraestrutura de tecnologia da informação de um cliente e os sistemas do usuário final. São contratados para executar um conjunto definido de serviços de gerenciamento diário, que podem incluir gerenciamento de rede e infraestrutura, segurança e monitoramento.

WTO/TBT, para o desenvolvimento de padrões internacionais, abordando as deficiências de segurança.

- Incluir componentes *OpenRAN* em esquema de certificação de segurança cibernética 5G.

Logo, identifica-se que, enquanto o relatório da UE tem um foco maior em aspectos de mais alto nível, o estudo do BSI possui uma abordagem mais técnica. Assim, para depois discorrer sobre os aspectos de gerenciamento e auditoria das redes abertas, este trabalho se debruça sobre ensaios de segurança que podem ser aplicados em redes de acesso abertas e verificar se são especificados pela O-RAN *Alliance*. Para tanto, foram levantadas duas referências[77] [78] que indicam requisitos de segurança que precisam ser avaliados para garantia de proteção à rede e aos usuários.

Ensaios relevantes para a verificação de segurança de redes de acesso em geral incluem *negative testing*, usado para verificar se há dados e condições de entrada inesperados no *software*, desde tipo de dados errado até ataque de *hackers*; *load testing*, usado para verificar o limite de dados processados pelo *software* até que ele não consiga mais processá-lo; *fuzzing*, que fornece dados aleatórios, inválidos ou inesperados como entradas para programas de computador, então monitorado, analisando exceções, como erros em tempo de execução; e *vulnerability scanning*, que analisa o alvo em busca de vulnerabilidades.

As especificações O-RAN *Alliance* possuem definidos ensaios específicos para estes itens nos documentos *O-RAN.SFG.Security-Test-Specifications-v02.00* (*fuzzing* e *vulnerability scanning*), *O-RAN.WG4.CONF.0-v05.00* (*negative testing*) e *O-RAN.TIFG.E2ETSTFWK.0-v01.00* (*load testing*).

Há também ensaios com enfoque em redes de acesso abertas como *open source software audit*, que analisa uma base de código proprietária usando uma combinação de ferramentas cuja entrega é um relatório que identifica o código aberto no código, bem como os riscos associados; *decision logic validations*, que verifica se as respostas de perguntas de lógica de decisão para cada modo de falha são válidas; e *apps policies/code review*, no qual aplicativos que devem ser publicados passam por uma revisão em que são verificados quanto à qualidade, correção e segurança do código.

Estes ensaios específicos para redes abertas também constam das especificações O-RAN *Alliance*, no documento *O-RAN.SFG.Security-Test-Specifications-v02.00*.

Outros pontos relevantes são a avaliação de risco, um termo usado para identificar, analisar e avaliar fatores de risco que têm o potencial de causar danos e a avaliação de postura de segurança cibernética, que verifica o status de segurança das redes, informações e sistemas com base nos recursos de segurança da informação e recursos existentes para gerenciar a defesa da empresa e reagir à medida que a situação muda. Ambos os itens são englobados nas especificações O-RAN *Alliance*, constando do documento *O-RAN threat model v03.00*.

[77] https://matrixshell.com/radio-access-network-security-assessment/
[78] https://www.indusface.com/blog/attributes-and-types-of-security-testing/

Porém, a literatura consultada recomenda também realização de ensaio de intrusão (*penetration testing* ou *pen-testing*) para avaliação de segurança de redes de acesso. *Pen-testing* é o processo de estimular um ataque cibernético em tempo real contra um alvo sob condições seguras. Ele deve ser executado manualmente por um especialista em segurança para entender a força das medidas de segurança contra ataques em tempo real e pode expor vulnerabilidades desconhecidas. *Pen-testing* pode ser executado em diferentes ambientes:

- Em *hardware* – o *pen-testing* de *hardware* envolve submeter partes selecionadas da infraestrutura de TI ao ensaio de intrusão. Ele pode se concentrar em dispositivos de Internet das Coisas (IoT), que inclui todos os dispositivos inteligentes e conectados à rede e tradicionalmente se concentram em *hardware* dentro de uma área definida, mas, dada a prevalência de soluções de computação em nuvem e móvel atualmente, ele também pode se concentrar em dispositivos usados remotamente.

- Na cadeia de suprimentos – necessário para garantir que os fornecedores também garantam a segurança na rede, com o ensaio em geral sendo executado por uma terceira parte.

- Na interface aérea – o *pen-testing* da interface aérea pode ser executado em redes do serviço móvel pessoal bem como em outras redes com interfaces sem fio, tais como wi-fi. Ele abrange a verificação da lista de vulnerabilidades de configuração, que podem permitir o uso ilegal de serviços nestas redes móveis.

- Na célula do serviço móvel – ERBs podem ser atacadas caso seja descoberto dispositivo para conexões externas, o que permite que um invasor alcance o transceptor da estação pela internet, por estouro de *buffer* de memória causado por pacotes UDP (*User Datagram Protocol*), uma falha de execução remota de código (RCE) que permite que o invasor execute código malicioso no dispositivo, ou caso um invasor consiga enviar tráfego de rotina para a estação. *Pen-testing* específico pode emular estes ataques com a finalidade de expor falhas de segurança e corrigi-las.

Como se pode ver, *pen-testing* tem relevância para identificar falhas de segurança em diferentes superfícies de ataque. A norma 3GPP TR 33 916 – *Security Assurance Methodology* (SECAM) chega a mencionar que pode ser necessário o uso de *pen-testing* para avaliar a resistência de uma rede quando da avaliação de vulnerabilidades, mas não o torna mandatório. Já as especificações O-RAN *Alliance* não mencionam *pen-testing*, que poderia aumentar a segurança e a resiliência de redes de acesso abertas.

Não obstante, por mais que as especificações O-RAN *Alliance* possuam requisitos avaliáveis de segurança, de acordo com o relatório do BSI estes não são mandatórios, o que poderia elevar a confiabilidade de redes baseadas na topologia *OpenRAN*.

Para além da segurança dos equipamentos e funções da RAN, o modelo de ameaça proposto na literatura consultada[79] apresenta como possíveis atores responsáveis por ameaças a redes de acesso abertas, que são classificados com base em seus padrões de engajamento com um potencial sistema *OpenRAN*, seja no estágio de *design* ou durante o estágio operacional, os seguintes agentes de ameaças, dentre outros:

Fabricante de *hardware*: sua capacidade contraditória é a de substituir componentes de *hardware* benignos por mal-intencionados. Essa atividade maliciosa pode operar de maneira independente ou pode ser controlada por uma entidade externa, como no caso de um *backdoor*. Esse agente de ameaças representa a dificuldade de resolver problemas da cadeia de suprimentos de *hardware* em que é impossível identificar componentes de *hardware* maliciosos de benignos.

Fornecedor de *hardware*: seja como integrador de sistemas ou como parte da cadeia de abastecimento de distribuição. Em termos de recursos contraditórios, um fornecedor de *hardware* tem acesso físico aos componentes de *hardware* usados pela rede aberta e tem os recursos para substituir componentes de *hardware* benignos por mal-intencionados. Além disso, no caso de um integrador de sistemas, o fornecedor também pode manipular o *firmware* e a pilha do sistema operacional. Deve-se notar que, em termos de recursos do invasor, uma grande diferença entre o fabricante de *hardware* e o fornecedor de *hardware* está enraizada na capacidade de um fabricante de implantar contramedidas de segurança que impedirão o fornecedor de executar uma ameaça.

Esta faceta identificada no estudo citado reforça a necessidade de se avaliar o processo produtivo de fornecedores de redes de acesso, nos moldes do esquema NESAS, conforme explicitado na subseção Avaliação de segurança em processos produtivos. Reforça-se que o Subgrupo Técnico de Equipamentos, Fornecedores e Requisitos do GT-Ciber da Anatel está trabalhando na elaboração de requisitos de avaliação de aspectos de segurança de fornecedores de telecomunicações.

Um sistema que pode servir como modelo para avaliação de segurança de processo produtivo de fornecedores é o desenvolvido pelo Escritório Federal de Segurança da Informação da Alemanha (BSI) baseado no esquema NESAS. Como já visto, o esquema NESAS descreve uma base global comum para a criação de requisitos nacionais e internacionais para a avaliação das características de segurança definidas dos equipamentos de rádio móveis. Apresentado em julho de 2022, este novo esquema do BSI para a certificação de segurança cibernética de componentes críticos usados em redes 5G é obrigatório[80]. Chama-se *NESAS Cybersecurity Certification Scheme – German Implementation* (NESAS CCS-GI). Este esquema nacional de certificação para equipamentos de rádio móvel 5G permite que os fabricantes demonstrem conformidade com as características de segurança necessárias por meio de um certificado de segurança de TI. Os fabricantes interessados podem enviar um pedido de

[79] Mimran, D. Bitton, R. Kfir, Y, Klevansky, E. Brodt, O. Lehmann, H. Elovici, Y. Shabtai, A. *Evaluating the Security of Open Radio Access Networks*; arXiv:2201.06080v1. https://doi.org/10.48550/arXiv.2201.06080

[80] https://www.cullen-international.com/client/site/documents/FLECDE20220001

certificação e os laboratórios de ensaio necessitam reconhecimento antes de realizar uma avaliação no campo do NESAS CCS-GI.

A diretiva técnica do BSI TR-03163[81] "Segurança em Infraestruturas de Telecomunicações" menciona o NESAS CCS-GI como um esquema admissível para a certificação de componentes críticos em redes de telecomunicações com maior potencial de risco, bem como instruções para a seleção de um regime de certificação adequado.

As sucessivas etapas de ensaio e os critérios de ensaio associados ajudam a avaliar o desempenho de segurança de TI dos componentes modernos de comunicações móveis. Ao adaptar os esquemas de avaliação existentes e participar de comitês internacionais, os requisitos nacionais para componentes certificados podem ser levados em conta, bem como os requisitos dos fabricantes globalmente ativos. O esquema NESAS CCS-GI complementa assim o portfólio existente do BSI com a Certificação de acordo com *Common Criteria*, a Certificação de acordo com as diretrizes técnicas e o Certificação de segurança acelerada.

Common Criteria é um padrão internacional para segurança de computadores. Este padrão é voltado para a segurança lógica das aplicações e para o desenvolvimento de aplicações seguras. Ele define um método para avaliação da segurança de ambientes de desenvolvimento de sistemas.

As Diretrizes Técnicas (TR) são utilizadas se, além da realização de determinadas propriedades de segurança, for necessário o cumprimento de requisitos funcionais para o funcionamento de um produto ou sistema de TI. Isto aplica-se, em particular, aos produtos e sistemas de TI destinados a serem utilizados em áreas soberanas.

A Certificação de Segurança Acelerada (BSZ) permite que os fabricantes tenham suas declarações de segurança relativas a um produto confirmado por um certificado independente. O regime de certificação associado baseia-se em tempos de avaliação previsíveis e mantém o esforço para o fabricante do produto - especialmente na área de documentação - gerenciável. A avaliação segue uma abordagem orientada ao risco que cria um alto nível de confiança nas declarações de segurança. O núcleo do BSZ é uma série de ensaios para determinar até que ponto o padrão de segurança prometido pelo fabricante é cumprido. Essas avaliações são realizadas em um prazo fixo, que depende da complexidade do produto. Os ensaios de conformidade são usados para confirmar a real provisão da garantia prometida. Os testes de intrusão (*pen-testing*) são então usados para examinar a eficácia das medidas técnicas de segurança/desempenho de segurança e as funções e procedimentos criptográficos utilizados no produto para erros típicos.

81 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03163/BSI-TR-03163.pdf?__blob=publicationFile&v=9

A Figura 32 - Guia de seleção do esquema de certificação, oriunda do anexo A[82] da diretiva BSI TR-03163, mostra a conexão entre as classes funcionais dos componentes 5G e os esquemas de certificação permitidos de acordo com a diretiva TR-03163. As linhas coloridas sólidas indicam as opções de certificação disponíveis. Uma linha tracejada significa que os documentos de requisitos estão em preparação pelo BSI.

A maioria dos componentes críticos da rede 5G executa funções de acordo com a arquitetura 3GPP. Esses componentes podem ser certificados usando NESAS CCS-GI. Além disso, os componentes críticos das conexões de rede podem ser certificados usando BSZ. Os Perfis de Proteção de *Common Criteria* (PP) estão em preparação para sistemas de gerenciamento NFV MANO e funções de rede principais fora das especificações 3GPP.

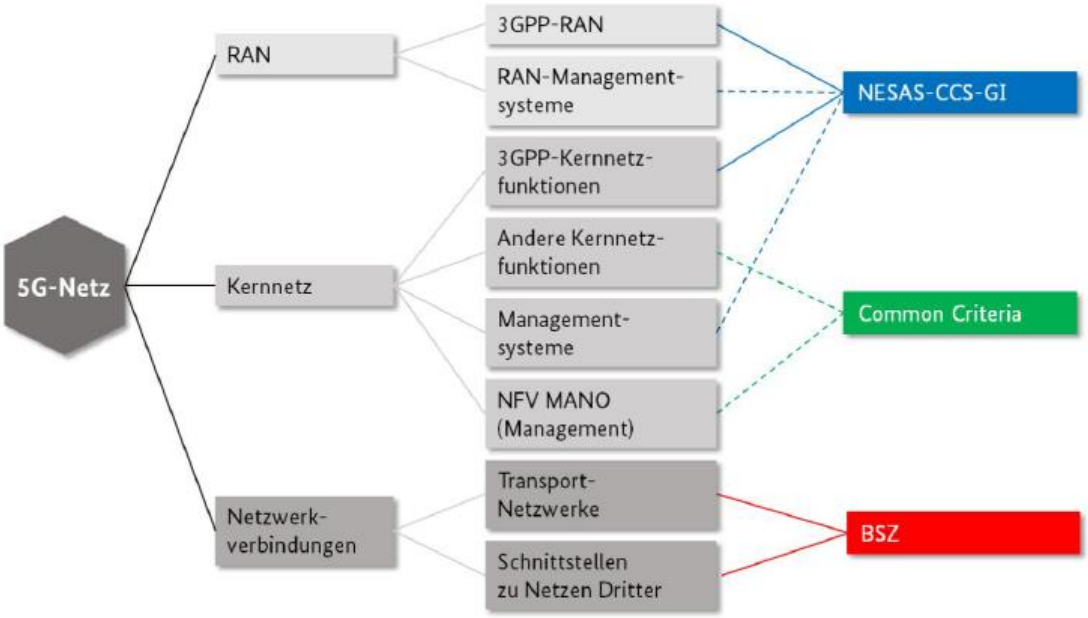

Figura 32 - Guia de seleção do esquema de certificação NESAS CCS-GI

Desta forma, sugere-se que a Anatel aprofunde os estudos realizados pela ORCN e pelo GT Ciber com relação a requisitos de segurança cibernética, notadamente um modelo de certificação de processos produtivos e possível adoção de princípios de segurança multilateral. Não obstante, este trabalho entende ser relevante a realização de *pen-testing* em redes de acesso, uma vez que as especificações do 3GPP e da O-RAN *Alliance* não preveem obrigatoriedade neste tipo de ensaio.

82 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03163/BSI-TR-03163_Anlage_A.pdf?__blob=publicationFile&v=9

8. CONCLUSÕES

8.1. Iniciativas Correlatas

O acompanhamento das ações do GT *OpenRAN* está disponível em sua página *online*. O detalhamento das iniciativas elaboradas pelo GT *OpenRAN*, incluindo proposições e conclusões, se encontra no Relatório de acompanhamento e avaliação da evolução de *OpenRAN*.

Além dos trabalhos e estudos realizados pelo GT *OpenRAN*, a Anatel tem desenvolvido outras ações com o intuito de aprofundar o conhecimento e as discussões sobre a topologia de redes abertas. Foram encaminhadas, e aceitas, contribuições da Agência a fóruns internacionais que têm discutido o tema, tais como OCDE, Citel e UIT. A Anatel também é membro do *steering board* do projeto OpenRAN@Brasil, liderado pelo Ministério da Ciência, Tecnologia e Inovação (MCTI) e conduzido pelo CPqD e pela Rede Nacional de Ensino e Pesquisa (RNP), e mantém interlocuções com o próprio MCTI e com o Ministério das Comunicações (MCom) sobre *OpenRAN*.

Vale ressaltar também o trabalho da Universidade de Brasília (UnB) que, por meio de Termo de Execução Descentralizada (TED), e com apoio da Universidade Federal de Goiás (UFG) e Instituto Federal do Ceará (IFCE), tem desenvolvido estudos sobre a topologia *OpenRAN* em três eixos, econômico, tecnológico e regulatório, que estão divididos em 10 subgrupos, nos quais a apresentação formal de resultados parciais está se realizando através de *workshops* que ocorrem bimestralmente desde outubro de 2022. Dentre os estudos em andamento, pode-se citar a elaboração e aceitação para apresentação em congressos de artigos sobre a capacitação de mão-de-obra e sobre experimentação de *OpenRAN* em plataformas de *software* aberto. O trabalho do TED tem previsão de conclusão em novembro de 2023 e seis relatórios parciais foram entregues:

- Relatório da meta 1 - Estudo sobre Estado da Arte do Open RAN aplicado ao Ecossistema de Telecomunicações Brasileiro.
- Relatório da meta 2 - Estudo Sobre Interoperabilidade e Perfis de Serviço no Open RAN.
- Relatório da meta 3 - Estudo sobre adequação de novas tecnologias aos conceitos Open RAN.
- Relatório da meta 7 - Estudo sobre valores agregados pelo Open RAN no mercado de serviços de telecomunicações brasileiro.
- Relatório da meta 8 - Estudo sobre necessidade de capacitação de mão de obra para o mercado nacional.
- Relatório da meta 9 - Estudo sobre eventuais barreiras legais e infralegais ao desenvolvimento do OPEN RAN.

Assim, o TED pode dar prosseguimento nos temas desenvolvidos no GT *OpenRAN*, aproveitando-se das discussões e dos estudos realizados. O eixo econômico e desenvolvimento de capital humano do TED pode aprofundar temas relacionados aos estudos descritos no Relatório de acompanhamento e avaliação da evolução de *OpenRAN*, a fim de verificar e confirmar os possíveis ganhos financeiros ao se adotar redes abertas, além de identificar as necessidades do mercado relacionadas à capacitação de mão-de-obra específica.

O eixo regulatório possui subgrupos de barreiras legais e infralegais e políticas públicas. Entre os temas de interesse, há especial atenção ao tema de patentes e direitos autorais.

O eixo tecnológico poderá acompanhar o desenvolvimento das especificações desenvolvidas pelos fóruns internacionais de *OpenRAN*, identificando as alterações e inclusões que estes documentos sofrerem e verificando a necessidade de ações regulatórias por parte da Anatel. Neste aspecto, salienta-se que, até então, não houve argumentação identificada que pudesse direcionar a Anatel a estabelecer requisitos de conformidade ou interoperabilidade a redes abertas, mas a Agência continuará acompanhando o mercado e interagindo com a equipe do TED caso alterações do mercado ou desenvolvimento de especificações apontem a necessidade de ações específicas da Agência.

O mesmo eixo tecnológico tem acompanhado os temas relacionados à segurança em *OpenRAN*. De acordo com a equipe do TED, os estudos têm confirmado que, comparando-se com as redes móveis 4G, as redes 5G sofreram aumento da superfície de ataque, o que poderia ser intensificado pela adoção da arquitetura *OpenRAN*. Os estudos no âmbito do eixo tecnológico também têm acompanhado as questões de virtualização de redes, além da integração e aumento do número de interfaces e fornecedores. Salienta-se que o subgrupo pretende criar ambiente experimental para avaliar casos prioritários, no qual poderia ser estudada a aplicação de *pen-testing* para avaliação de segurança de redes abertas.

Outra ação desenvolvida pela equipe do TED relacionada a Cibersegurança foi a produção de artigo científico apresentado em congresso nacional com o título “Open RAN e os desafios de sua experimentação em plataformas de código aberto”, no qual se discute os principais desafios nas plataformas de código aberto de pesquisa experimentais que podem ser usadas para projetar e avaliar a virtualização, desagregação e uso de interfaces não proprietárias previstas para redes abertas (SEI nº 9024282).

Salienta-se também que as equipes dos GTs Ciber e *OpenRAN* e dos TEDs Ciber (centralizada na Universidade Federal de Campina Grande, UFCG) e *OpenRAN* têm interagido entre si, de tal sorte que a sinergia de esforços permite expandir as pesquisas e identificar possibilidades de ações conjuntas, sendo um exemplo a apresentação realizada no 2º *Workshop* TED Segurança Cibernética 5G, em 15 de agosto de 2022, no qual foi exposto um panorama evolutivo do 4G/LTE e 5G com relação à arquitetura *OpenRAN* e segurança cibernética.

8.2. Comentários Finais

Com fundamento na Análise nº 13/2021/CB (SEI nº 6500863), foi criado o Grupo de Estudos/Trabalho sobre *OpenRAN* (GT *OpenRAN*), sob coordenação da Superintendência de Outorga e Recursos à Prestação. O GT *OpenRAN* tem como objetivo estudar o tema relativos às redes de acesso abertas e os demais aspectos referentes à interoperabilidade entre equipamentos de diferentes fornecedores, acompanhando e avaliando as ações que estão ocorrendo em outros países e no mercado.

A arquitetura *OpenRAN* (*Open Radio Access Network*, Rede Aberta de Acesso via Rádio) visa permitir que uma determinada empresa que queira implementar uma operação de rede de telecomunicações baseada em tecnologia 5G possa implementá-la com elementos de variados fornecedores de equipamentos.

No âmbito dos trabalhos do GT *OpenRAN*, foi elaborado Relatório técnico final de acompanhamento e avaliação da evolução de *OpenRAN*, que resume as discussões realizadas e as conclusões obtidas durantes os estudos do grupo. O Relatório visa relatar e avaliar a evolução da arquitetura *OpenRAN*, a fim de subsidiar o desenho da próxima Agenda Regulatória, com objetivo de expor a necessidade de ações, em âmbito regulatório, que possam habilitar os potenciais efeitos positivos da arquitetura *OpenRAN*.

Quanto às questões relativas à interoperabilidade, considerando os estudos do GT concluiu-se que os requisitos estabelecidos pelo 3GPP, O-RAN *Alliance* e *Small Cell Forum*, por exemplo, são suficientes para garantir interoperabilidade. Ainda que as especificações desenvolvidas pelos fóruns temáticos citados ainda não cubram todas as características necessárias para garantirem a conformidade e a interoperabilidade de quaisquer módulos e unidades *OpenRAN*, tais especificações estão sendo definidas e fornecidas conforme são finalizadas, o que permite à Anatel direcionar sua atenção a outras áreas de interesse.

No processo de certificação e homologação, entende-se, até este momento, não ser necessária a avaliação da interoperabilidade dos protocolos de comunicação utilizados nas interfaces internas entre os elementos de uma rede de telecomunicações. Salienta-se que, até então, não houve argumentação identificada que pudesse direcionar a Anatel a estabelecer requisitos de conformidade ou interoperabilidade a redes abertas, mas a Agência continuará acompanhando o mercado e interagindo com a equipe do TED caso alterações do mercado ou desenvolvimento de especificações apontem a necessidade de ações específicas da Agência.

Destaca-se que, caso a Anatel decidisse por estabelecer requisitos de certificação de forma a garantir a aderência dos equipamentos aos protocolos de comunicação padronizados pelos fóruns internacionais em referência, isso seria uma mudança de paradigma de grande impacto interno, na medida que iria exigir a elaboração de todo um arcabouço regulatório de requisitos específicos para essa finalidade. Em complemento, é importante frisar que essa mudança de paradigma iria demandar mais tempo para conclusão dos processos de certificação e homologação de equipamentos, além de encarecer os respectivos custos.

O desenvolvimento do ecossistema *OpenRAN* em âmbito mundial ainda está nos seus estágios iniciais, com poucas operações comerciais relevantes, e ainda há muita discussão nos respectivos fóruns internacionais a respeito da padronização das interfaces vinculadas à *OpenRAN*.

Portanto, no atual contexto, entende-se que o mais prudente seria a Anatel seguir acompanhando a evolução deste ecossistema, sem impor, nesse momento, requisitos específicos de certificação de interoperabilidade entre elementos internos de redes de telecomunicações.

A respeito dos quesitos de segurança, cabe observar que há preocupações de que a abordagem atualmente utilizada para garantia de segurança em redes de acesso, baseada em confiança nos procedimentos, controle de acesso de usuário e defesa de perímetro, não seja apropriada para as redes atuais, em especial *OpenRANs*. Como estas são mais abertas do que as RANs monolíticas e, a princípio, podem possuir mais superfície de ataque, a sua política de segurança deve garantir que possíveis vulnerabilidades sejam expostas e tratadas a contento.

Da mesma forma que no processo de certificação e homologação a Anatel não avalia a interoperabilidade dos protocolos de comunicação utilizados nas interfaces internas entre os elementos de uma rede de telecomunicações, presentemente, também não é avaliada a segurança de tais protocolos, ou o grau de robustez dos equipamentos de telecomunicações para mitigar ataques cibernéticos.

Compreende-se que a avaliação da segurança cibernética em produtos difere da avaliação da conformidade já realizada pela Anatel por meio do processo de certificação dos produtos. O processo de certificação atualmente aplicado pela Agência realiza avaliações de parâmetros determinísticos, cujo comportamento não se altera no decorrer do tempo, tais como: máxima potência de transmissão, largura de banda e emissões espúrias de radiofrequência. Para todos esses parâmetros são conhecidos os limites máximo e mínimo para atendimento dos requisitos e quais os procedimentos de ensaios padronizados aplicáveis para sua verificação. Já a avaliação de segurança cibernética é realizada sobre parâmetros dinâmicos: a cada dia são descobertas novas vulnerabilidades em produtos ou agentes mal-intencionados desenvolvem novas técnicas para explorar funcionalidades de equipamentos que, até aquele momento, eram consideradas seguras.

Em uma primeira avaliação, entendeu-se que a padronização em desenvolvimento para os equipamentos *OpenRAN* irá endereçar de forma adequada os problemas de segurança identificados nesta nova arquitetura e em seus equipamentos. Destaca-se, neste contexto, que não há requisitos de segurança cibernética mandatórios nas especificações desenvolvidas pelos fóruns temáticos.

A respeito desse tema, a Anatel emitiu a Resolução nº 740 de 21 de dezembro de 2020 – Aprova o Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações. Este Regulamento está focado em regular a atuação dos prestadores de serviços de telecomunicações, de forma a mitigar riscos de danos por ataques cibernéticos às suas respectivas redes. Adicionalmente, cumpre destacar que, em janeiro de 2021, a Agência publicou o Ato nº 77, de 05 de janeiro de 2021, que aprovou

os Requisitos de Segurança Cibernética para Equipamentos para Telecomunicações. Este documento apresenta um conjunto de recomendações de segurança que fabricantes e fornecedores de equipamentos devem adotar no ciclo de vida de seus produtos, desde a concepção, aplicando-se o conceito de *security-by-design*, até a fase de vendas e suporte ao consumidor, adotando estratégias de identificação e correção de vulnerabilidades em produtos já disponíveis no mercado.

Desta forma, a Agência tem estado atenta ao tema e caso se identifique, no decorrer da implantação e do uso da nova tecnologia, que determinadas características ou vulnerabilidades já conhecidas devam ser endereçadas no processo de certificação dos equipamentos para *OpenRAN*, a Agência, por meio de sua Superintendência competente, poderá definir requisitos mandatórios para avaliação da segurança cibernética destes equipamentos, sempre de forma alinhada às recomendações e *frameworks* adotados internacionalmente, a fim de não criar barreiras técnicas para a introdução dos produtos no país.

Feitas as considerações anteriores, entende-se que, até este momento, não se faz necessária alteração a nível político-regulatório para endereçar questões relativas à segurança da rede. De toda forma, vale frisar que a Anatel já estabeleceu um Grupo Técnico específico para tratar de segurança cibernética de redes de telecomunicações – o Grupo Técnico de Segurança Cibernética e Gestão de Riscos de Infraestrutura Crítica (GT-Ciber). Portanto, entende-se importante a continuidade dos estudos e discussões para avaliação de eventuais próximos passos que venham a ser necessários em relação ao tema de segurança.

No âmbito das discussões sobre redes de acesso, cabe observar também que o mercado de telecomunicações móveis brasileiro possui três grandes prestadoras do serviço móvel pessoal em escala nacional, além de algumas prestadoras regionais. As prestadoras nacionais são empresas multinacionais e realizam compras de equipamentos baseadas em suas ações globais. Desta forma, supõe-se que, pelo menos em um primeiro momento, tais entidades possam não adotar o uso de *OpenRAN* em larga escala. Não obstante, por não haver ainda confirmações de benefícios econômicos propagados pelo mercado quanto à adoção da topologia *OpenRAN*, além de possível carência de mão-de-obra especializada, prestadoras regionais e locais podem se sentir desestimuladas à implantação de redes de acesso abertas em sua infraestrutura, pelo menos enquanto não se superam esses dois pontos.

Além dos aspectos resumidos acima, cabe mencionar as iniciativas da Agência que, direta ou indiretamente, podem estimular o desenvolvimento e a expansão de redes de acesso, em especial, aquelas associadas ao serviço móvel pessoal. Dentre tais iniciativas, destacam-se os estudos para eventual possibilidade de uso de sistemas IMT na faixa de 4,9 GHz. Adicionalmente, cumpre mencionar que se espera a ampliação de implementação de redes de acesso também no âmbito das redes privativas, considerando a regulamentação de diferentes faixas de frequências para este propósito, como por exemplo, das faixas de 3,7 GHz a 3,8 GHz e 27,5 GHz a 27,9 GHz.

Destaca-se ainda as ações relativas à simplificação dos processos de licenciamento, estabelecido pelo regulamento aprovado pela Resolução nº 719/2020 e as diretrizes

trazidas pelo Regulamento de Numeração de Serviços de Telecomunicações, aprovado pela Resolução nº 749/2022, que dispensa do uso de numeração pública por estações M2M (*machine to machine communications*, comunicação máquina-a-máquina) e IoT, por exemplo, que podem estimular o desenvolvimento de redes de acesso e, por consequência, redes com arquitetura *OpenRAN*.

Cabe destacar também que, considerando que os equipamentos a serem utilizados no contexto da implementação de redes com arquitetura *OpenRAN* podem necessitar de testes antes da submissão dos equipamentos a procedimentos de certificação e homologação, as iniciativas da Agência no sentido de introduzir a possibilidade regulatória relativa ao Ambiente Regulatório Experimental (*Sandbox* Regulatório), além da atualização das diretrizes relacionadas ao uso temporário do espectro, apresentada à sociedade por meio da Consulta Pública nº 41/2022, podem favorecer também o andamento da implementação de redes com arquitetura *OpenRAN* no Brasil. Neste contexto, vale observar a importância de que o acesso ao uso da hipótese do *Sandbox* Regulatório seja dinâmico o suficiente para permitir que os projetos interessados possam usufruir desta possibilidade de forma tempestiva, a fim de permitir maior dinamismo ao desenvolvimento tecnológico.

ANATEL
Agência Nacional de Telecomunicações