Universidade de Brasília

Instituto de Ciências Exatas Departamento de Ciência da Computação

Pós-Graduação em Computação Aplicada - PPCA

Avaliação das Infraestruturas Críticas das Redes de Cabos ópticos submarinos no Brasil

CLÁUDIO SILVA DE OLIVEIRA

Monografia apresentada ao Departamento de Ciência da Computação da Universidade de Brasília como requisito parcial para a conclusão do Mestrado profissional em Computação Aplicada (MCPA): Programa de Computação Aplicada.

Orientador

Professor Dr. João Mello da Silva

Brasília

2021

CLÁUDIO SILVA DE OLIVEIRA

Avaliação das Infraestruturas Críticas das Redes de Cabos ópticos Submarinos no Brasil.

Monografia apresentada ao Departamento de Ciência da Computação da Universidade de Brasília como requisito parcial para a obtenção do título de Mestre em Computação Aplicada (MCPA): Programa de Computação Aplicada.

Orientador
Professor Dr. João Mello da Silva
Universidade de Brasília

Brasília, 22 de setembro de 2021.

Ficha catalográfica elaborada automaticamente,
com os dados fornecidos pelo(a) autor(a)

Oliveira, Cláudio Silva de
OO48a Avaliação das Infraestruturas Críticas das Redes de Cabos ópticos submarinos no Brasil / Cláudio Silva de Oliveira; orientador João Mello da Silva. -- Brasília, 2021.
84 p.

Dissertação (Mestrado - Mestrado Profissional em Computação Aplicada) -- Universidade de Brasília, 2021.

1. Infraestruturas Críticas. 2. Gestão de Riscos. 3. Redes de Telecomunicações. I. Silva, João Mello da, orient. II. Título.

Ata de Defesa de Monografia

Monografia de Especialização Stricto Sensu, defendida sob o título *Avaliação das Infraestruturas Críticas das Redes de Cabos ópticos Submarinos no Brasil,* por Cláudio Silva de Oliveira, em 22 de setembro de 2021, por meio de teleconferência realizada na plataforma *Teams* da UNB, em Brasília - DF, e aprovada pela banca examinadora constituída por:

Prof. Dr. João Mello da Silva
Universidade de Brasília - UNB
Orientador

Prof. Dr. João Gabriel de Moraes Souza
Universidade de Brasília – UNB
Examinador Interno

Prof. Dr. Edgard Costa Oliveira
Universidade de Brasília – UNB
Examinador Interno

Dr. Paulo Eduardo dos Reis Cardoso
Agência Nacional de Telecomunicações - Anatel
Examinador Externo

Dedicatória

Dedico aos meus Pais que souberam me conduzir durante todas as fases de minha vida! À minha esposa Vanessa Cimino, pela paciência em meus momentos de ausência, por sua capacidade de me trazer paz e amor ao longo de nossa vida. Dedico também a todos os professores do Mestrado, em especial ao Dr. João Mello da Silva pelo conhecimento transmitido e apoio nas horas mais difíceis.

Agradecimentos

À Deus, que se mostrou criador, que foi criativo. Seu fôlego de vida em mim, sustentou-me e me encorajou para questionar realidades e propor sempre um novo mundo de possibilidades.

A todos os professores do curso, que foram tão importantes na minha vida acadêmica e no desenvolvimento desta monografia.

À Vanessa Cimino, esposa, amiga, companheira, pessoa com quem amo partilhar a vida. Com você tenho me sentido mais vivo. Obrigado pelo carinho, a paciência e por sua capacidade de me trazer paz e amor ao longo de nossa vida.

Aos amigos e colegas, pelo incentivo e pelo apoio constante. Aos colegas de curso da UNB, e às pessoas com quem convivi nesses espaços ao longo desses anos. A experiência de uma produção compartilhada na comunhão com amigos nesses espaços foram a melhor experiência da minha formação acadêmica.

A todos aqueles que de alguma forma estiveram e estão próximos a mim, fazendo esta vida valer cada vez mais a pena.

"*Quem chega cedo ao campo de batalha*
aguarda a chegada do inimigo e está pronto para combater.
Quem chega tarde ao campo de batalha tem que apressar-se e
já começa o combate com as forças exauridas."
Sun Tzu, em *A Arte da Guerra*

RESUMO

O presente trabalho tem por objetivo propor a Avaliação do Cenário Atual da Gestão de Riscos nas Redes de Cabos Submarinos Brasileiras com intuito de antecipar-se com ações Proativas para melhor adequação aos Normativos e Regulamentos presentes na Agência que permeiam àquelas Redes para Garantir maior Desempenho, Disponibilidade e Qualidade para os Usuários de Telecomunicações. Por meio do presente trabalho serão determinados o contexto interno e externo para que em uma próxima etapa possam ser identificados, avaliados e tratados os riscos envolvidos em tal processo por meio de ferramentas específicas descritas na ISO 31000.

Palavras-chave: Gestão de Risco; Cabos Submarinos; Infraestrutura Crítica; ISO 31000;Contexto Interno e Externo.

ABSTRACT

This study aims to propose a scenario evaluation Current Risk Management in Cable Networks Submarines Brazilian in order to anticipate with actions proactive to better match the Normative and these Regulations within the Agency that permeate those networks to ensure greater performance, availability and quality for the Telecommunications Users. Through this work will be determined the internal and external context so that in a next step can be identified, evaluated and addressed the risks involved in this process through specific tools described in ISO 31000.

Key words: Risk management; Subsea cables; Critical Infrastructure; ISO 31000: Internal and External Context.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

GSI Gestão da segurança da informação.

GTSIC Grupo Técnico de Segurança de Infraestrutura Crítica das Telecomunicações.

Anatel Agência Nacional de Telecomunicações.

LGT Lei Geral de Telecomunicações.

Funttel Desenvolvimento Tecnológico das Telecomunicações.

PICT Projeto Proteção de Infraestrutura Crítica de Telecomunicações.

TEMAC Teoria de Enfoque Meta Analítico Consolidado.

WoS Web of Science.

FIFA Federação Internacional de Futebol Associada.

CREDEN Câmara de Relações Exteriores e Defesa Nacional.

GTSIC Grupo Técnico de Segurança de Infraestruturas Críticas.

GSIPR Segurança Institucional da Presidência da República.

CODI Gerência de Controle de Obrigações de Direitos dos Consumidores.

COQL Gerência de Controle de Obrigações de Qualidade.

COUN Gerência de Controle de Obrigações de Universalização e de Ampliação do Acesso.

COGE Gerência de Controle de Obrigações Gerais.

PDTI Plano Diretor de Tecnologia da Informação.

SLTE Terminais de Linha Submarinos.

DWDM Dense Wavelength Division Multiplexing

DCN Data Communications Network.

POP Pontos de Presença.

NOC Network Operation.

ISO Internacional Organization for Standardization.

SIEC Sistema de Infraestrutura Criticas das Redes de Telecomunicações na Anatel.

AAF Análise de Árvore de Falha.

FTA Fault Tree Analysis.

AMFE Análise de Modos de Falhas e Efeitos

FMEA Failure Modes and Effect Analysis.

AAE Análise de Árvore de Eventos.

ETA Event Tree Analysis.

CAPÍTULO 1

1. INTRODUÇÃO

1.1. DELIMITAÇÃO DO PROBLEMA

A segurança da informação tem o intuito de preservar as características da informação no que concerne principalmente à sua disponibilidade, confidencialidade e integridade. A preservação dessas características depende do estabelecimento de uma ação gerencial explícita, que é chamada de gestão da segurança da informação (GSI).

Consideram-se Infraestruturas Críticas das Comunicações, conforme portaria nº 5 do Gabinete de Segurança Institucional, de 27 de janeiro de 2009, as instalações, serviços, bens e sistemas que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança do Estado e da sociedade.

Infraestrutura crítica das telecomunicações é peça que deve ser considerada quando trata das questões de segurança, proteção contra riscos e é um setor intensivo em capital e tecnologia, obsolescência acelerada e necessita competência para sua administração. Cada vez mais ela se integra em todas as atividades da vida humana e das sociedades, aproximando-se do setor de tecnologia da informação e comunicação. (TAKAYANAGY, NELSON)

A abertura do mercado de telecomunicações gerou nos últimos vinte anos, uma onda - sem precedentes - de investimentos nas estradas de informação submarina na América Latina. A rede de cabos que interconectam o Brasil com os outros países transporta boa parte das informações entre o País e o resto do mundo por meio dessa estrutura.

Recentemente as denúncias de espionagem contra autoridades e empresas brasileiras causaram mal-estar nas relações entre Estados Unidos e Brasil, por um lado, mas também evidenciaram um problema de segurança nacional: o País mostrou-se um alvo fácil na guerra cibernética.

Telecomunicações é um setor necessariamente envolvido nas relações internacionais, para garantir adequada operação, proteção contra-ataques cibernéticos e acesso a tecnologias de ponta.

É oportuno e conveniente avaliar e ajustar, se necessário, a atual legislação brasileira no que tange à proteção das Infraestruturas de Telecomunicações, em especial, à das redes de cabos submarinos em território nacional.

1.2. CONTEXTUALIZAÇÃO

Dentre as ações estratégicas para contribuir com o incremento do nível de segurança nacional estão as medidas para a segurança das áreas de infraestruturas críticas, incluindo os serviços, em especial no que se refere à energia, transportes, água e telecomunicações, a cargo dos Ministérios da Defesa, das Minas e Energia, dos Transportes, da Integração Nacional e das Comunicações, e ao trabalho de coordenação, avaliação, monitoramento e redução de riscos, desempenhado pelo Gabinete de Segurança Institucional da Presidência da República (GSI/PR).

Na Portaria nº 2, de 8 de fevereiro de 2008 do Gabinete de Segurança Institucional da Presidência da República (GSIPR) estão definidas as atribuições dos GTSICs. A Portaria Interministerial nº 16 – GSIPR/CH, de 18 de julho de 2008, assinada pelo Ministro de Estado Chefe do Gabinete de Segurança Institucional da Presidência da República e pelo Ministro de Estado das Comunicações, instituiu à época o Grupo Técnico de Segurança de Infraestrutura Crítica das Telecomunicações (GTSIC – Telecom) composto pelo GSIPR, Ministério das Comunicações, Agência Nacional de Telecomunicações (Anatel) e outros órgãos e especialistas convidados pelo GTSIC – Telecom.

O Gabinete de Segurança Institucional da Presidência da República instituiu o Subgrupo Técnico de Segurança de Infraestruturas Críticas de Radiodifusão (SGTSIC – Radiodifusão) e o Subgrupo Técnico de Segurança de Infraestruturas Críticas de Telecomunicações (SGTSIC – Telecomunicações), por meio das Portarias nº 4 e 5 – GSIPR/CH, de 27 de janeiro de 2009.

Já no âmbito internacional, o tema infraestruturas críticas já vêm sendo discutido amplamente. Em 2004, foi aprovada, pelas Nações Unidas, a Resolução UN 58/199 sobre a “Proteção da infraestrutura crítica da informação”.

Desta forma, observa-se que o tema Segurança de Infraestruturas Críticas nas Telecomunicações tem sido amplamente discutido em âmbito nacional e internacional. Até meados de 2013 o setor de telecomunicações brasileiro não possuía uma estrutura interna para gerenciar os riscos associados às redes e serviços de telecomunicações. Portanto, mostrava-se necessária a atuação nesta área, evidenciado pela necessidade trazida pelos Grandes Eventos Internacionais

(Copa do Mundo e Jogos Olímpicos), quando eventuais ataques às redes se tornam mais propensos e a administração de riscos passa a ser imperativa. Destaca-se também a necessidade de manutenção da qualidade dos serviços, mitigando possibilidade de interrupções e bloqueio, com uma gestão aprimorada e eficaz, com o desenvolvimento da solução que atenda os anseios do setor.

Fernandes e Rodrigues (2013) apresentam os conceitos da cibernética, da teoria dos sistemas e das redes complexas; os processos de trabalho, normas e riscos concomitantemente criados no interior das organizações humanas; o impacto da introdução das tecnologias de informação e comunicação nos processos de trabalho das organizações humanas; o surgimento das infraestruturas críticas e a necessidade de sua proteção, segurança e defesa; a abordagem de engenharia de segurança; os fenômenos do *hacking* e do *cracking*; as características do crime organizado na Internet; a ocorrência dos incidentes de segurança que pode conduzir às crises organizacionais; e, por fim, o sistema normativo de Gestão de SIC em desenvolvimento no país.

Fernandes e Rodrigues (2013) propõem uma pesquisa de estudo de caso na investigação da aplicação do processo de trabalho racional na gestão de SIC das organizações públicas federais do Brasil.

Argumentam ainda que a Segurança da Informação e Comunicações - SIC, desenvolvida na Administração Pública Federal brasileira, considera a natureza complexa e distribuída dos órgãos e instituições federais, muitos deles com estruturas geograficamente distribuídas no território nacional, e cujas ações são pautadas pela transparência e intensa relação com a sociedade.

A Segurança da Informação é definida como a “proteção dos ativos de informação de uma organização contra muitas ameaças, visando assegurar ou garantir a continuidade das atividades de negócio ou o cumprimento da missão crítica desta organização, minimizando os riscos às suas atividades, maximizando retorno sobre seus investimentos e as oportunidades de sucesso”.

De forma bastante simplificada, infraestruturas críticas são artefatos tecnológicos fundamentais usados por um sistema viável, ou dos quais ele depende.

A Agência Nacional de Telecomunicações (Anatel) é uma autarquia especial criada pela Lei Geral de Telecomunicações (LGT) - Lei 9.472, de 16 de julho de 1997, administrativamente independente, financeiramente autônoma e sem subordinação hierárquica a nenhum órgão de governo.

A missão da Anatel é promover o desenvolvimento das telecomunicações do País de modo a dotá-lo de uma moderna e eficiente infraestrutura de telecomunicações, capaz de oferecer à sociedade serviços adequados, diversificados e a preços justos, em todo o território nacional.

A Agência herdou, do Ministério das Comunicações, os poderes de outorga, regulamentação e fiscalização, além de um grande acervo técnico e patrimonial. Compete à Anatel adotar as medidas necessárias para o atendimento do interesse público e para o desenvolvimento das telecomunicações brasileiras, atuando com independência, imparcialidade, legalidade, impessoalidade e publicidade.

São normas do código de conduta dos servidores da Anatel, dentre outras: a) Zelar pelo patrimônio da Anatel, inclusive pela utilização cuidadosa e adequada dos equipamentos e materiais, destinados à execução de suas atividades; b) Preservar o sigilo de informações privilegiadas das quais tenha conhecimento.

Na Anatel o tema de Infraestrutura Crítica na área das Telecomunicações já vem sendo tratado há alguns anos. A Portaria da Anatel nº 222, de 12 de março de 2007, criou Grupo de Trabalho para tratar deste tema, em função do projeto de Proteção de Infraestrutura Crítica de Telecomunicações (PICT), que foi executado pela Fundação CPqD, no período de 2007 até 2009, com recursos do Fundo para o Desenvolvimento Tecnológico das Telecomunicações (Funttel).

Em meados de 2009, o projeto Proteção de Infraestrutura Crítica de Telecomunicações (PICT), financiado pelo Fundo para o Desenvolvimento Tecnológico das Telecomunicações (Funttel), desenvolvido pelo CPqD e coordenado pela Anatel, abrangeu a elaboração, validação e aplicação de um conjunto de metodologias, culminando com a formulação de recomendações para a proteção de infraestrutura crítica de telecomunicações no Brasil.

A primeira etapa do projeto consistiu na determinação dos elementos críticos da infraestrutura de telecomunicações brasileiras, com a aplicação da Metodologia de identificação de Infraestrutura Crítica. Outra etapa deste projeto consistiu na elaboração da Metodologia para a Identificação e Análise de Ameaças, que abordou o levantamento, a análise e a determinação das ameaças que poderiam causar danos à infraestrutura crítica.

O projeto PICT procurou identificar a Infraestrutura Crítica de Telecomunicações no escopo dos jogos Pan-Americanos de 2007 e ao planejamento da segurança da infraestrutura de telecomunicações utilizado durante os XV Jogos Pan-americanos.

Apesar de inovador o projeto PICT não abrangeu todas as infraestruturas de redes e serviços de telecomunicações no País, era preciso um novo projeto que pudesse abarcar essa necessidade da Agência. Já no primeiro semestre de 2012, deu início na Agência o levantamento das necessidades e elaboração de um projeto básico que pudesse suprir esta deficiência.

Uma Solução para gerenciamento do risco das redes e serviços de telecomunicações do País foi contratada pela Agência em dezembro de 2012, por meio de pregão eletrônico. A referida solução encontra-se em fase de implementação, mas precisamente na etapa de confecção do módulo de avaliação e gerenciamento de redes.

De acordo com o Termo de Referência da Contratação, a gestão de riscos será feita de acordo com a norma ABNT NBR ISO 31000:2009 – Gestão de riscos – princípios e diretrizes. O primeiro passo foi a elaboração de um inventário dos ativos que tem seus riscos analisados. Devido à enorme quantidade de ativos de telecomunicações existentes no país, fez-se necessário a priorização os ativos mais relevantes ou estratégicos, que serão objeto da gestão de riscos. Estimou-se que o número de ativos estratégicos é em torno de 5.000 (cinco mil). Os ativos que darão suporte aos grandes eventos esportivos internacionais fizeram parte deste rol.

O módulo de monitoramento das redes de telecomunicações, em fase de implantação, destina-se a permitir que o regulador obtenha informações periodicamente do estado das redes, bem como formar um histórico das condições das redes. O módulo de redes da solução deverá estar integrado com os módulos de gestão de risco de forma a permitir a troca de dados sobre os eventos relevantes ocorridos nas redes que possam influenciar no nível de risco das redes e serviços de telecomunicações.

Recentemente a Anatel passou por um processo de reestruturação no qual teve o objetivo de melhorar os processos internos de trabalho, facilitando assim a interação entre as áreas, permitindo aumento na produtividade.

Dentre as novas Superintendências criadas, a Superintendência de Controle de Obrigações é responsável pelo acompanhamento da solução adquirida no final de 2012 para gerenciar os riscos e monitorar a qualidade das Infraestruturas Críticas das Redes de Telecomunicações no País.

1.3. A ANATEL

A Agência Nacional de Telecomunicações (Anatel) é uma autarquia especial criada pela Lei Geral de Telecomunicações (LGT) - Lei 9.472, de 16 de julho de 1997, administrativamente independente, financeiramente autônoma e sem subordinação hierárquica a nenhum órgão de governo.

A missão da Anatel é promover o desenvolvimento das telecomunicações do País de modo a dotá-lo de uma moderna e eficiente infraestrutura de telecomunicações, capaz de oferecer à sociedade serviços adequados, diversificados e a preços justos, em todo o território nacional.

A Agência herdou, do Ministério das Comunicações, os poderes de outorga, regulamentação e fiscalização, além de um grande acervo técnico e patrimonial. Compete à Anatel adotar as medidas necessárias para o atendimento do interesse público e para o desenvolvimento das telecomunicações brasileiras, atuando com independência, imparcialidade, legalidade, impessoalidade e publicidade.

São normas do código de conduta dos servidores da Anatel, dentre outras: a) Zelar pelo patrimônio da Anatel, inclusive pela utilização cuidadosa e adequada dos equipamentos e materiais, destinados à execução de suas atividades; b) Preservar o sigilo de informações privilegiadas das quais tenha conhecimento.

Na Anatel o tema de Infraestrutura Crítica na área das Telecomunicações já vem sendo tratado há alguns anos.

Recentemente a Anatel passou por um processo de reestruturação no qual teve o objetivo de melhorar os processos internos de trabalho, facilitando assim, a interação entre as áreas, permitindo aumento na produtividade.

Dentre as novas Superintendências criadas, a Superintendência de Controle de Obrigações é responsável pelo acompanhamento da solução adquirida no final de 2012 para gerenciar os riscos e monitorar a qualidade das Infraestruturas Críticas das Redes de Telecomunicações no País.

Até o primeiro semestre de 2013, a Anatel não avaliava, de forma sistemática, o risco de segurança associado às infraestruturas críticas de telecomunicações. Além do mais, não há normas dentro da Agência que estabeleçam requisitos para o gerenciamento dos riscos relacionados à segurança das infraestruturas críticas de telecomunicações.

OBJETIVOS DA GESTÃO DE RISCOS NA ANATEL: estabelecer definições, procedimentos e condutas para a promoção da disponibilidade, da segurança e do

desempenho das redes e serviços de telecomunicações de interesse coletivo, em especial quando da ocorrência de desastres e emergências, ou sua iminência, mediante:

I - adoção de medidas para acompanhamento do desempenho das redes;

II - adoção de processo de gestão de riscos das infraestruturas críticas de telecomunicações; e,

III - estabelecimento de medidas de preparação e de resposta para desastre, situação de emergência ou estado de calamidade pública.

CAPÍTULO 2

2. LEVANTAMENTO DO ESTADO DA ARTE

A revisão da bibliografia é a principal base para se obter uma boa pesquisa em um trabalho científico (MARIANO et al., 2011). Antes de iniciar uma pesquisa específica, o pesquisador deve averiguar o que já se sabe sobre o fenômeno estudado para produzir um estudo que agregue conhecimento à temática (GARCIA; RAMIREZ, 2005). O estabelecimento do referencial teórico para este trabalho foi construído utilizando a Teoria de Enfoque Meta Analítico Consolidado – TEMAC, de Mariano e Rocha (2017). Essa técnica de revisão bibliográfica tem como objetivo selecionar materiais confiáveis de maneira sistemática, para identificar o estado da arte sobre o assunto, as principais linhas de pesquisa e as respectivas abordagens teóricas. O TEMAC é fundamentado em três etapas: a preparação da pesquisa; a apresentação e inter-relação dos dados; e o detalhamento, modelo integrador e validação por evidências.

As três etapas supracitadas foram então aplicadas, conforme descrito no decorrer deste capítulo. As buscas se deram entre os dias de 19 a 22 de junho de 2020.

2.1. Etapa 1: Preparação da pesquisa

Segundo Mariano e Rocha (2017), na primeira etapa o pesquisador deve responder a quatro perguntas essenciais para direcionar a pesquisa:

A. Quais bases de dados serão utilizadas?
B. Qual o descritor, string ou palavra-chave de pesquisa?
C. Quais áreas de conhecimento serão utilizadas?
D. Qual o campo espaço-tempo da pesquisa?

Foi definido como *string* de busca “*submarine cable*”. Optou-se pela base de dados *Web of Science - WoS* (www.webofknowledge.com) por ser reconhecida internacionalmente como uma das mais importantes plataformas online de pesquisa para acesso a bases de dados bibliográficos (GARCÍA; RAMIREZ, 2005), e porque a base do WoS também acessa artigos disponíveis em outras bases, como o Scopus, ProQuest e Wiley, publicados em periódicos indexados e classificados segundo fator de impacto no *Jornal Citation Reports* (JCR).

Como a base escolhida oferece periódicos e artigos científicos sobre o tema a partir do ano 2000, o espaço temporal foi definido pelo intervalo entre os anos de 2000 a 2020, pois a partir do ano 2000 iniciou-se as implantações das atuais redes de cabos submarinos no Brasil, além de obter-se um maior raio temporal possível. Em relação às áreas do conhecimento, optou-se por filtrar categorias relacionadas às Engenharias, Ciência da Computação, Redes óticas e Telecomunicações, visto que são áreas correlatas ao tema e também se faz presente em um vasto campo de aplicação e a pesquisa tem a intenção de identificar os estudos mais significativos, independente da área em que se enquadrem. A busca foi realizada entre os dias 19 a 22 de junho de 2020 e retornou um total de 288 registros com média de 4,83 citações por item, o que evidencia um médio índice de relevância da literatura analisada. Nos últimos anos a quantidade de publicações e citações cresceu de forma expressiva, evidenciando a importância do assunto e a sua tendência de crescimento. Os maiores índices de citações ocorreram nos anos de 2018 e 2019, evidenciando uma relevância atual ao tema.

2.1.1. Etapa 2: apresentação e inter-relação dos dados

Nesta segunda etapa, foram realizadas as inter-relações entre os dados dos registros encontrados, as leis de bibliometria, como a Lei de Brandford, que mensura a relevância de um periódico em uma determinada área de conhecimento, a Lei do Elitismo e Lei do 80/20, que apresentam as maiores representatividades (elite) de um determinado tema, Lei de Lokta, que justifica que uma larga proporção da literatura científica é produzida por um pequeno número de autores, e a Lei da Obsolescência da Literatura, que estima o declínio dos registros em determinada área de conhecimento (MARIANO; ROCHA, 2017), chegando aos resultados a seguir expostos.

2.1.1.1. Áreas e subáreas que mais publicam sobre o tema

Em relação às áreas de pesquisa, os 288 artigos coletados se encontram subdivididos entre seguintes áreas de pesquisa escolhidos: *engineering electrical electronic, energy fuels, telecommunications, optics, computer science theory methods. Robotics e computer science information systems*, das quais 18 com pelo menos dois documentos, o que demostra a abrangência do tema estudado. A Figura 1 apresenta as 10 principais áreas em termos quantitativos de publicação.

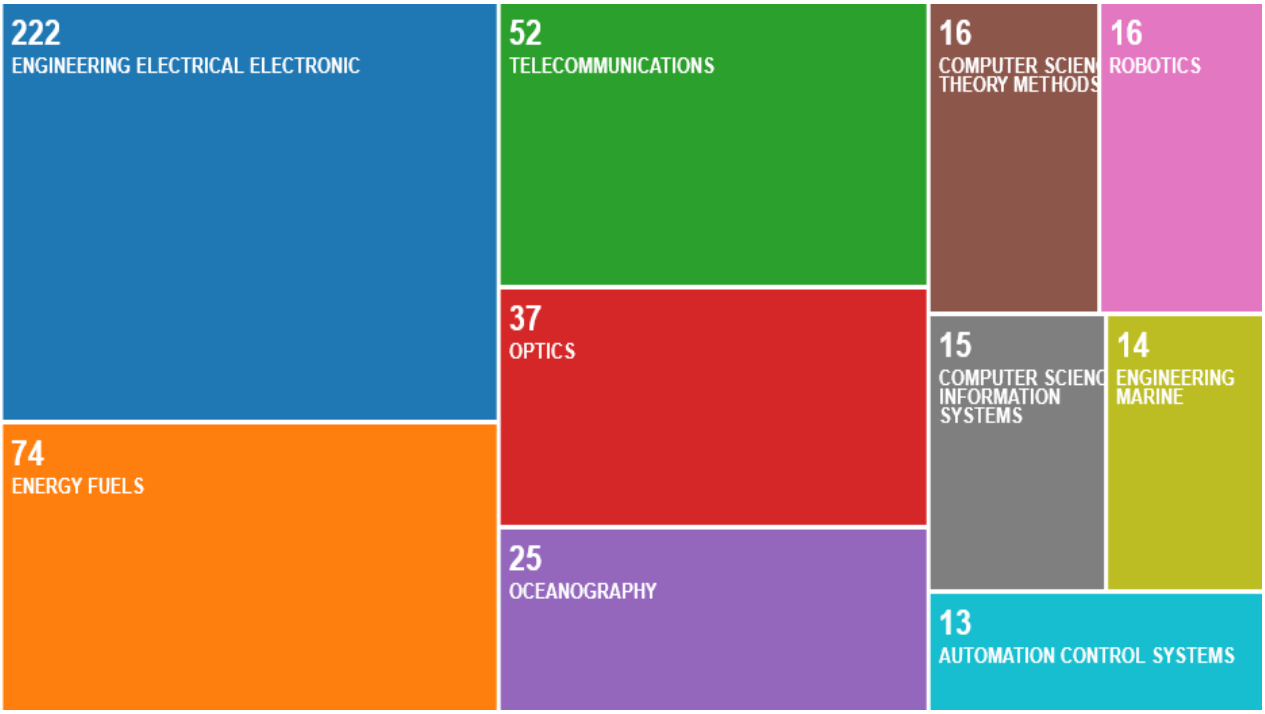


Figura 1 Principais áreas de Publicação.

Nota-se que existem três áreas principais*: Engineering Electrical Electronic*, (222) que corresponde a 77% das publicações; *Energy Fuels* (74) que corresponde a cerca de 30% dos dados; e *telecommunications* (52) cerca de 18% dos dados. Vale ressaltar que um artigo pode ser classificado em diversas áreas de conhecimento, o que justifica o somatório das porcentagens dos documentos ultrapassar 100%.

2.1.1.2. Seleção das revistas que mais publicam sobre o tema

Nesta etapa foram encontrados 25 grupos de revistas que publicam dois ou mais artigos sobre o tema. O Quadro 1 traz as dez revistas principais, de acordo com quantitativo de publicações presente na base WoS.

Posição	Fonte de Publicação	Registros	Percentual
1	IEEE TRANSACTIONS ON POWER DELIVERY	13	4.514%
2	2007 SYMPOSIUM ON UNDERWATER TECHNC	9	3.125%
3	IEEE POWER AND ENERGY SOCIETY GENERAL	9	3.125%
4	JOURNAL OF LIGHTWAVE TECHNOLOGY	9	3.125%
5	IEEE JOURNAL OF OCEANIC ENGINEERING	7	2.431%
6	OCEANS IEEE	7	2.431%
7	ENERGIES	6	2.083%
8	IEEE ACCESS	5	1.736%
9	CONFERENCE ON ELECTRICAL INSULATION A	4	1.389%
10	ELECTRIC POWER SYSTEMS RESEARCH	4	1.389%

Quadro 1 Publicações Relevantes.

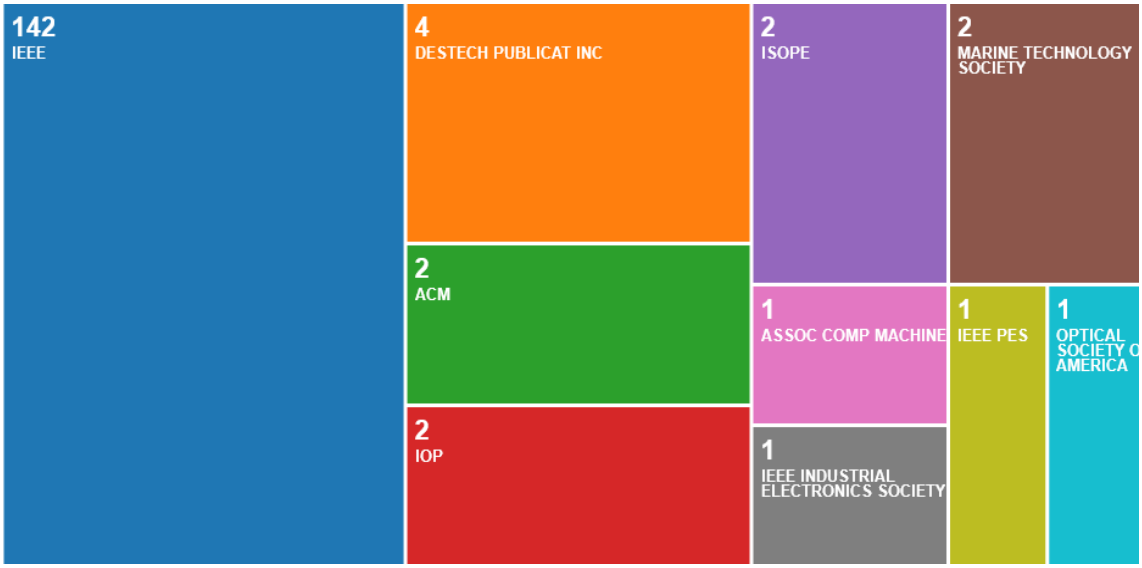


Figura 2 Principais Publicadores.

O IEEE aparece como sendo a principal fonte de publicação do tema no período escolhido, com 142 registros, equivalente a 49% das publicações.

2.1.1.3. Evolução do tema ano a ano

A evolução do tema a nível mundial, no que se refere ao número de publicações e citações entre o período de 2000 a 2020, é apresentado nas Figuras 3 e 4 respectivamente.

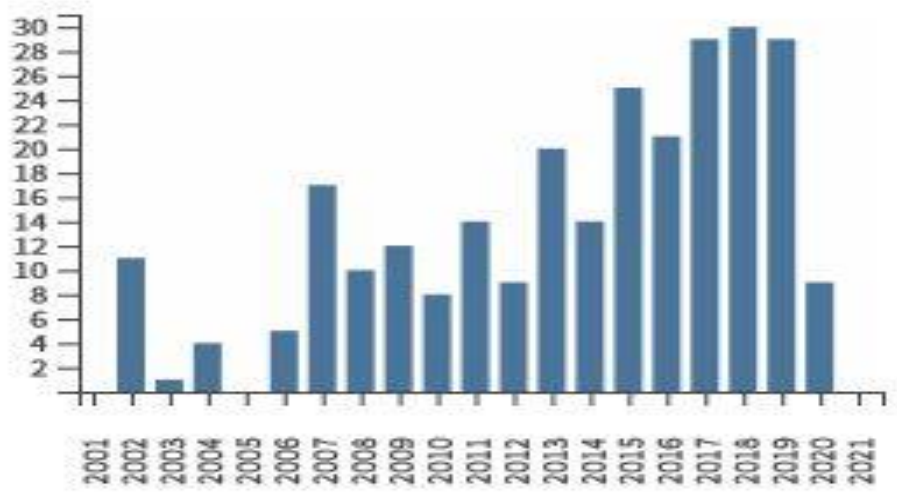


Figura 3 Quantitativo de publicações sobre o tema no decorrer dos anos.

Percebe-se com base na Figura 3 acima que o quantitativo de publicações sobre o tema vem crescendo nos últimos 3 anos e teve o maior pico em 2018.

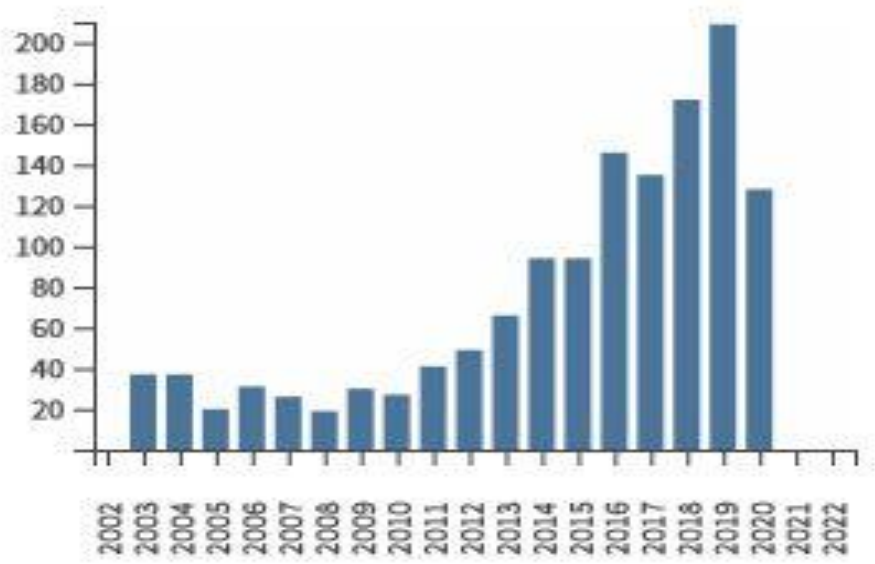


Figura 4 Citações no decorrer dos anos.

Em relação ao quantitativo de citação, o tema apresentou uma evolução quase exponencial a partir de 2015, conforme Figura 4. Os 288 documentos encontrados receberam maior número de citação no ano de 2018, o que demonstra que o interesse recente pelo tema.

Através dos dois gráficos apresentados, pode-se verificar que o tema referente à Cabos Submarinos vem ganhando interesse científico ano a ano, visto que o

número de publicações e citações aumentaram de forma expressiva recentemente nos últimos 4 anos.

2.1.1.4. Países e organizações que mais publicam

Foram encontrados 18 países que publicaram sobre o tema. Os países que mais pesquisaram estão elencados no gráfico constante da Figura 5.

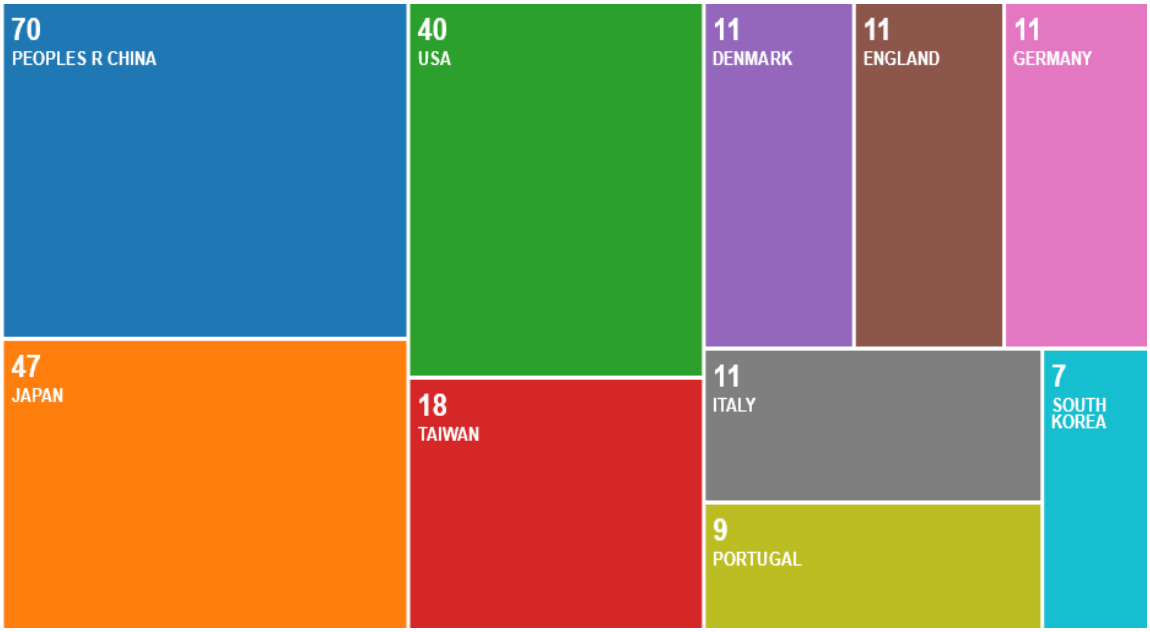


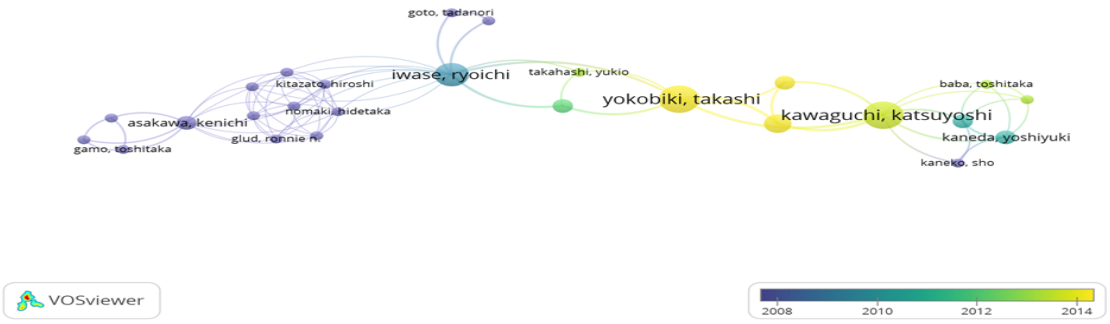
Figura 5 Países que publicaram sobre o tema.

Pode-se observar que a China, Japão e Estados Unidos com 157 registros aparecem como os principais países em termos de publicações. Foram encontradas 3 publicações realizadas no Brasil.

2.1.1.5. Artigos mais citados

Entre os 15 artigos mais citados, 2 tem relação com o objeto da pesquisa. Os demais abordam em sua maioria informações de métodos alternativos de energia para serem empregados nas redes de cabos submarinos ou ainda fazem abordagem de redes ópticas, ou até sobre a utilização de cabos submarinos desativados para realização de análises geográficas. Os dois artigos referenciados e aderentes ao tema são: *Measuring the Resilience of the Trans-Oceanic Telecommunication Cable System e Experience with restoration of Asia Pacific network failures from Taiwan earthquake*. O segundo aborda a experiência com restauração de falhas de rede da

Ásia-Pacífico devido ao terremoto de Taiwan enquanto o primeiro trata da resiliência do sistema de cabo de telecomunicações transoceânico.



2.1.2. Etapa 3: detalhamento das análises

Para aprofundar a pesquisa bibliográfica, foram realizadas, nesta etapa, as análises bibliométricas de co-ocorrência de palavras-chave, de co-citação e de *coupling* (acoplamento bibliográfico). Essas análises, segundo Zupic e Cater (2015), são utilizadas para mapear a ciência, introduzindo uma medida de objetividade na avaliação da literatura científica, de modo a aumentar o rigor e mitigar o viés do pesquisador no estudo. A co-ocorrência das principais palavras-chave evidencia linhas de pesquisa. A análise de co-citação traz uma perspectiva das abordagens mais utilizadas, a visão do passado, enquanto a de *coupling* revela as frentes de pesquisa, uma perspectiva de futuro. Para a geração dos mapas de calor utilizou-se o *software VOSviewer* versão1.6.8

Co-ocorrência de palavras-chave: estrutura conceitual do campo

Para identificar a estrutura conceitual sobre o tema estudado, realizou-se a análise deco-words, uma técnica de análise de conteúdo que usa as palavras-chave de maior ocorrência nos documentos selecionados para construir a rede de temas e suas relações, que representam a estrutura conceitual do campo. Diferente das análises de citações, co-citação e acoplamento bibliográfico, que conectam documentos indiretamente através de citações, a análise de cowords usa o conteúdo real dos documentos para construir uma medida de similaridade (ZUPIC; CATER, 2015). A ideia subjacente ao método é que quando as palavras co-ocorrem com

frequência nos documentos, significa que os conceitos por trás dessas palavras estão intimamente relacionados.

A Figura 6 retrata, de forma visual, a estrutura conceitual em torno da temática das redes de Cabos Submarinos, considerando palavras-chave e títulos dos 288 documentos coletados na base WoS, que foram extraídos e exportados para o *software VOSviewer* para geração do mapa de calor.

É possível verificar que há núcleos no mapa de calor que apresentam as palavras chave, indicando a similaridade de tema. Observa-se que se agrupam junto ao conceito central de Cabos submarinos, as palavras-chave frequência, fibra óptica, performance, topologia (designer), perda de potência, tensão de recuperação.

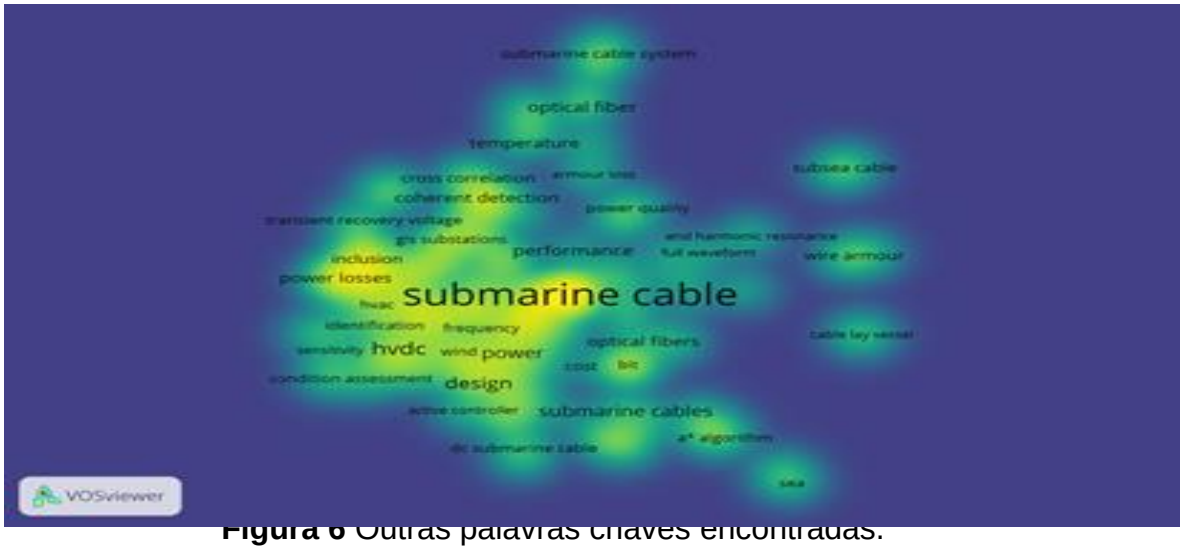


Figura 6 Outras palavras chaves encontradas.

2.1.2.1. Análises Co-citação

De acordo com Zupic e Cater (2015), sintetizar os achados históricos é uma das mais importantes tarefas para conseguir avançar numa linha de pesquisa específica. Esses autores destacam a análise de co-citação dentre os inúmeros métodos existentes para alcançar esse objetivo.

Considerando que nenhum método substitui a análise do pesquisador, buscaram-se pelos artigos mais citados pela amostra, apresentados na Figura 7. Os mesmos são explorados pelo pesquisador para conclusões mais robustas e assertivas.

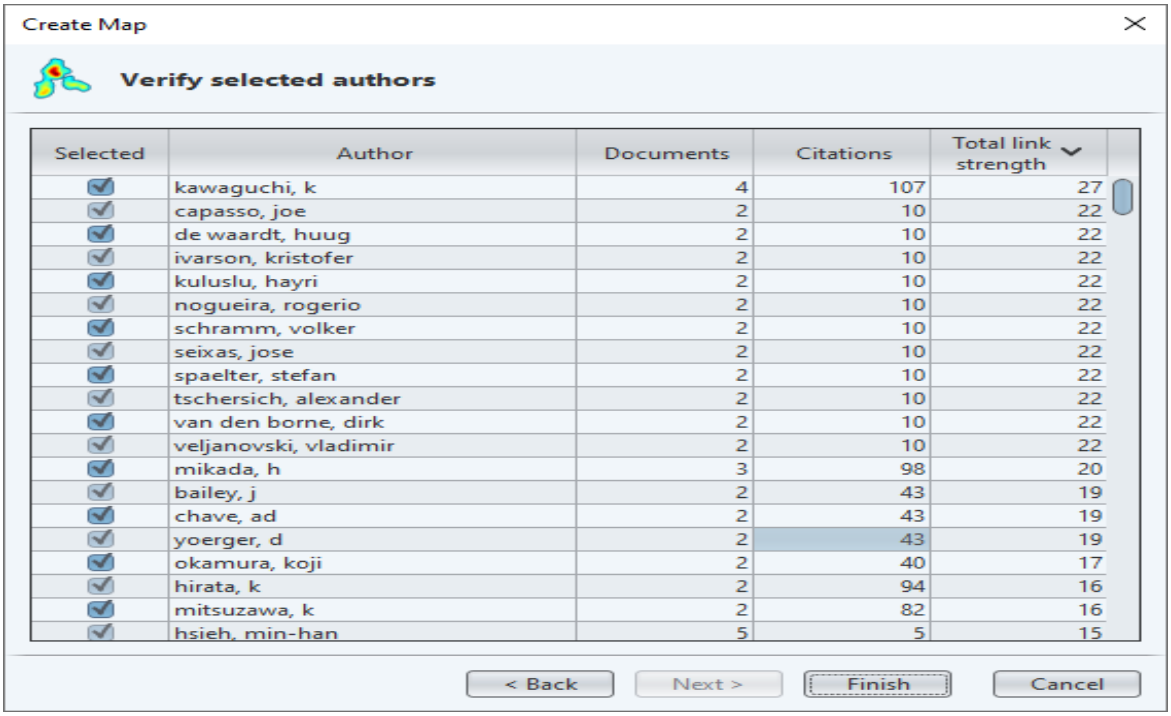


Figura 7 Amostra de artigos.

A Figura 8 retrata o mapa de calor de co-citação para o período de 2000 a 2020. 231 artigos receberam pelo menos 5 citações pelos 288 artigos da amostra, gerando o mapa de calor. Os mais citados estão representados pelas maiores fontes e situam-se nos centros das manchas de calor.

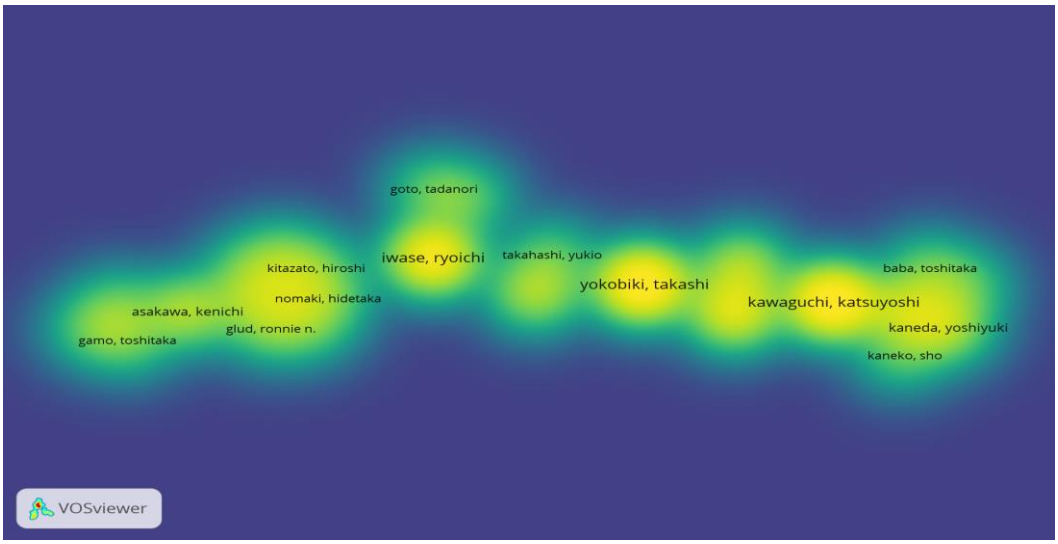


Figura 8 Mapa de Calor co-citação.

2.1.2.2. Análise de Coupling – frentes de pesquisa

Enquanto a co-citação traz uma perspectiva de abordagens voltadas para o passado, a análise bibliográfica Coupling tem como objetivo identificar as principais frentes de pesquisas a que se está dedicando atualmente (COBO et al., 2012), apontando as tendências de futuro.

Para isso, os artigos foram tabulados no software VOSviewer, sendo selecionados os artigos que receberam pelo menos 5 citações nos últimos 3 anos e os autores que mais foram citados são apresentados no mapa de calor da Figura 10.

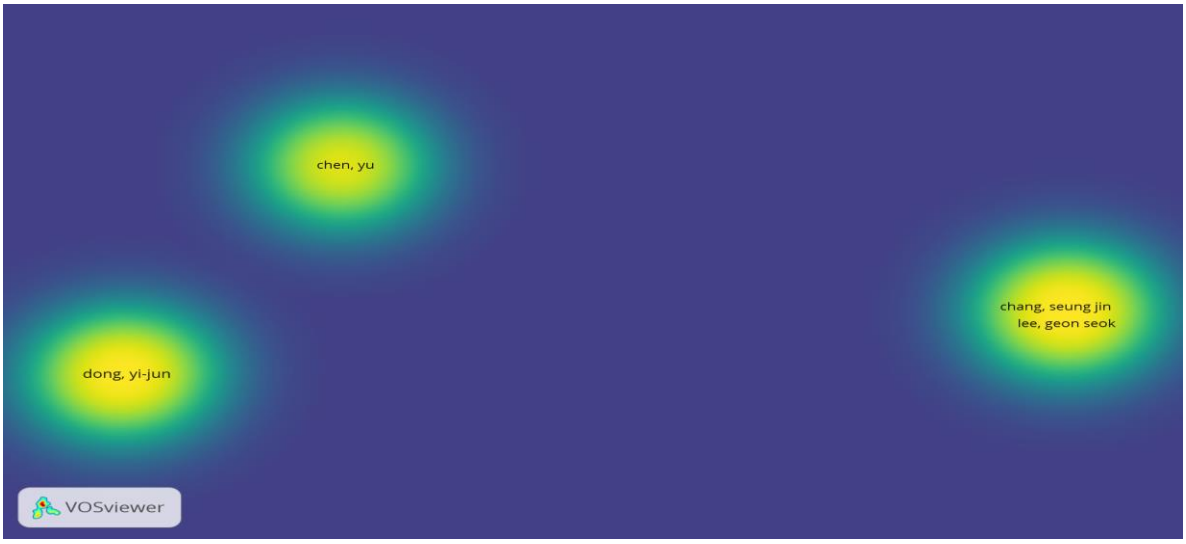


Figura 9 Mapa de Calor últimos 3 anos.

Com o objetivo de obter abordagens mais atualizadas, por meio das análises de *Co-occurrence* e *Coupling*, refinou-se a busca para os últimos 3 anos, mantendo o mesmo termo de busca definido inicialmente. A busca retornou uma amostra de 60 publicações que corresponde a cerca de 20% da amostra inicial.

Da leitura do resumo dos artigos levantados com a utilização da TEMAC, foram selecionados para leitura e análise os seguintes artigos:

Título 1: *Measuring the Resilience of the Trans-Oceanic Telecommunication Cable System*

Autores: Omer, Mayada; Nilchiani, Roshanak; Mostashari, Ali

Titulo 2*: Experience with restoration of Asia Pacific network failures from Taiwan earthquake*

Autores: Kitamura, Yasuichi; Lee, Youngseok; Sakiyama, Ryo; Okamura, Koji

CAPÍTULO 3

3.1. CONTEXTO EXTERNO

O Governo Federal assinou compromissos com a FIFA – Federação Internacional de Futebol Associada, em 2007, dentro do processo de escolha do país que iria sediar a Copa de 2014. Neste acordo, o país se comprometeu em atender 11 obrigações que iam desde isenções tributárias, questões trabalhistas, segurança, proteção e aspectos de telecomunicações e tecnologia da informação. A 11ª garantia assinada pelo Governo Federal para este Grande Evento Internacional visava garantir a segurança e o uso das redes e serviços de telecomunicações de interesse coletivo por modernos sistemas e tecnologias atualizados, disponibilizados e apropriados para a demanda da Copa.

Em atendimento às necessidades apresentadas pela FIFA e pela União, a Anatel criou à época um Grupo de Trabalho (GT) para os Grandes Eventos Internacionais, formalizado pela Portaria nº 470, de 2 de junho de 2011. Esse Grupo de Trabalho foi criado com o intuito de assessorar o Conselho Diretor da Anatel na gestão da infraestrutura para os Grandes Eventos Internacionais compreendidos entre 2011 e 2016, incluindo no âmbito dos trabalhos a Copa das Confederações de 2013, a Copa do Mundo em 2014 e as Olimpíadas de 2016.

No âmbito do Governo Federal, o tema da Segurança das Infraestruturas Críticas também foi tratado por vários órgãos. A Câmara de Relações Exteriores e Defesa Nacional (CREDEN) instituiu o Grupo Técnico de Segurança de Infraestruturas Críticas (GTSIC) para estudar e propor a implementação de medidas e de ações relacionadas com a segurança das infraestruturas críticas nas áreas de energia, transporte, água e telecomunicações, por meio da Resolução nº 2, de 24 de outubro de 2007.

A Portaria nº 2, de 8 de fevereiro de 2008 do Gabinete de Segurança Institucional da Presidência da República (GSIPR) definiu as atribuições dos GTSICs. A Portaria Interministerial nº 16 – GSIPR/CH, de 18 de julho de 2008, assinada pelo Ministro de Estado Chefe do Gabinete de Segurança Institucional da Presidência da República e pelo Ministro de Estado das Comunicações, instituiu o Grupo Técnico de Segurança de Infraestrutura Crítica das Telecomunicações (GTSIC – Telecom) composto pelo GSIPR, Ministério das Comunicações, Agência Nacional de

Telecomunicações (Anatel) e outros órgãos e especialistas convidados pelo GTSIC – Telecom.

O Gabinete de Segurança Institucional da Presidência da República instituiu o Subgrupo Técnico de Segurança de Infraestruturas Críticas de Radiodifusão (SGTSIC – Radiodifusão) e o Subgrupo Técnico de Segurança de Infraestruturas Críticas de Telecomunicações (SGTSIC – Telecomunicações).

No âmbito internacional, o tema infraestruturas críticas já vêm sendo discutido. Em 2004, foi aprovada, pelas Nações Unidas, a Resolução UN 58/199 sobre a “Proteção da infraestrutura crítica da informação”.

Um levantamento junto a 337 instituições federais, feito pelo Tribunal de Contas da União (TCU) em 2012, mostrou que houve melhora no tratamento da segurança da informação em relação a 2010. Mesmo assim, alguns índices continuam muito baixos. Os percentuais relacionados à designação de equipe para gerenciamento da segurança da informação e à formalização de política de segurança da informação tiveram crescimento razoável, 11% e 12%, respectivamente.

Por outro lado, alguns itens de segurança sofreram retrocesso: inventário de ativos de informação, análise de riscos e gestão de incidentes. "Causa preocupação especial o baixo percentual de instituições que realizam análise de risco, o qual caiu de 17% para 10%. Ou seja, 90% das instituições públicas federais ainda não realizavam esse tipo de análise", alertou o TCU, conforme figura 11:

Figura 10 Ambiente Inseguro.

Sumariamente o Contexto Externo baseia-se na Disponibilidade das Redes de Cabos Submarinos com foco em três elementos chaves: Prestadoras Outorgadas do Serviço de Comunicação Multimídia, Usuários destes serviços e Órgãos de Controle Externo/Interno, conforme exposto na figura 12:

Figura 11 Contexto Externo

3.2. CONTEXTO *INTERNO*

3.2.1. Estrutura Organizacional e Força de Trabalho

A Anatel possui sua estrutura composta de diversos órgãos cujas atribuições mais recentes estão amplamente descritas na Resolução nº 612, de 29 de abril de 2013. Abaixo, descrevemos resumidamente tais órgãos:

- **Conselho Consultivo (CC):** é o órgão de participação da sociedade na Anatel, sendo composto por representantes indicados pelo Senado Federal. Seus membros não são remunerados e tem como atribuições principais apreciar, aconselhar e opinar a respeito das políticas governamentais e proposições relevantes da Agência;
- **Conselho Diretor (CD):** Os membros do conselho diretor são responsáveis pela aprovação dos principais planos e produtos da Agência, incluindo normas de licitação, diretrizes gerais e plano estratégico da Agência, contratação de pessoal, entre muitos outros;
- **Presidência (PR):** A presidência da Anatel é exercida pelo Presidente do Conselho Diretor, cabendo-lhe nessa qualidade o comando hierárquico sobre o pessoal e o serviço de toda a Agência, exercendo todas as competências administrativas correspondentes ao cargo;
- **Ouvidoria (OV):** é um órgão com atuação independente (sem vinculação hierárquica ao CD) com acesso a todos os assuntos internos e cuja função é fazer apreciações críticas sobre a atuação da Agência;

- **Secretariado do Conselho Diretor (SCD):** tem como competência organizar e secretariar os Fóruns de Decisão e as reuniões técnicas de apresentação para o Conselho Diretor, bem como zelar pela administração das atividades inerentes ao Conselho Diretor e ao Conselho Consultivo
- **Gabinete da Presidência (GPR):** tem como competência zelar pela administração das atividades inerentes à Presidência da Agência, elaborando a agenda, organizando e assessorando-o no relacionamento com os órgãos, autoridades e os agentes públicos da Anatel, bem como nos contatos externos;
- **Superintendente Executivo (SUE):** tem como competência auxiliar o Presidente no exercício de suas funções executivas e coordenar a realização de atividades que lhe forem atribuídas pelo Presidente e pelo Conselho Diretor;
- **Auditoria Interna (AUD):** A auditoria interna tem como competência avaliar a eficiência e eficácia dos controles internos, visando garantir a salvaguarda dos ativos, a fidedignidade dos dados operacionais, contábeis, orçamentários, financeiros e patrimoniais, o cumprimento das leis, dos regulamentos e demais instrumentos normativos estabelecidos, a melhoria da eficiência operacional e a eficiência e economia na aplicação dos recursos;
- **Procuradoria Federal Especializada (PFE):** órgão de execução da Procuradoria-Geral Federal, vinculada à Advocacia-Geral da União para fins de orientação normativa e supervisão técnica, dirigida por um Procurador-Geral tem como competência representar judicialmente a Agência, apurar a liquidez e certeza dos créditos, de qualquer natureza, inerentes às suas atividades, inscrevendo-os em dívida ativa, para fins de cobrança amigável ou judicial, executar as atividades de consultoria e assessoramento jurídicos, emitindo pareceres, notas, informações, cotas e despachos;
- **Assessorias:** são órgãos subordinados ao Presidente com competências diversas.
- **Corregedoria (CRG):** tem como competência apurar denúncias ou representações envolvendo servidores da Agência, instaurar sindicâncias e processos administrativos disciplinares, incluindo indicação de procedimentos

de correição, e emitir parecer sobre desempenho de servidores para confirmação no cargo ou exoneração;

- **Órgãos executivos (Superintendências):** atualmente são 8 Superintendências subordinadas funcionalmente ao Conselho Diretor e administrativamente ao Presidente e tem diferentes funções, conforme detalhado mais adiante

Um resumo do descrito acima pode ser visualizado na figura 12.

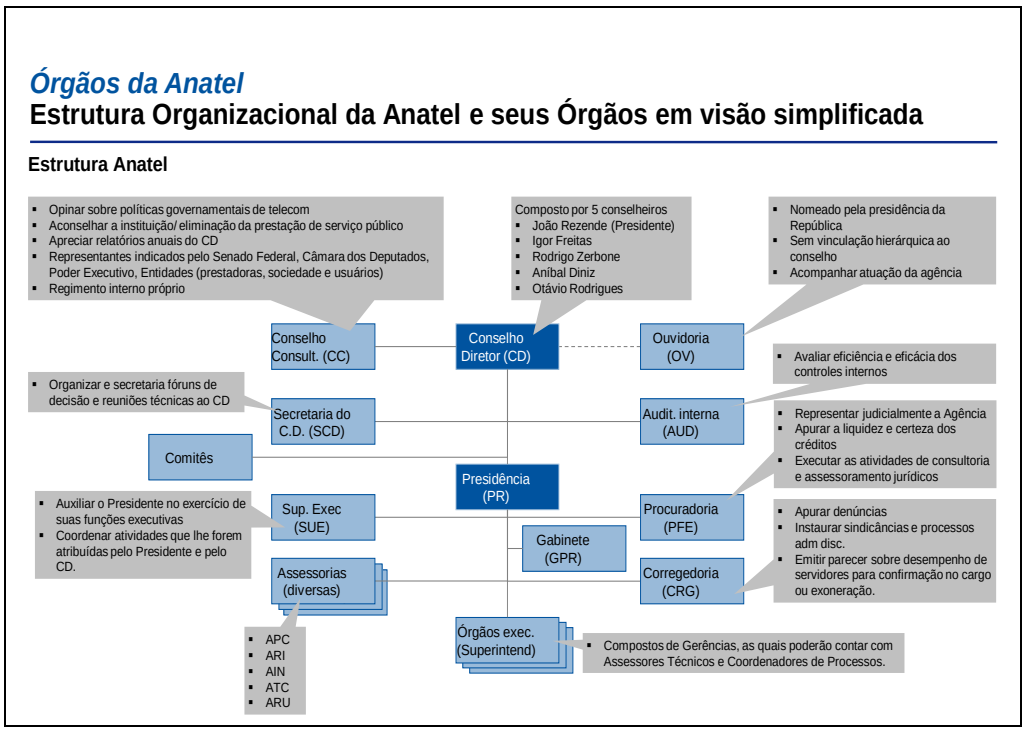


Figura 12 Estrutura Organizacional da Anatel resumida.

Os órgãos executivos estão organizados em gerências conforme abaixo:

- Superintendência de Planejamento e Regulamentação (SPR): tem como competência temas como, propor e submeter à aprovação as diretrizes gerais, plano estratégico, regulamentações, entre outros.
- Superintendência de Outorga e Recursos à Prestação (SOR): tem como competência temas como, a realização de processos de licitação para outorgar concessão, permissão e autorização para a exploração de serviços, certificar e homologar produtos.
- Superintendência de Controle de Obrigações (SCO): tem como competência temas como, acompanhar e controlar as obrigações das detentoras de concessão, permissão e autorização para exploração de serviços de

telecomunicações, acompanhar e controlar Termo de Ajustamento de Conduta, entre outros. É composta pelas seguintes gerências:

  - Gerência de Controle de Obrigações de Direitos dos Consumidores (CODI)
  - Gerência de Controle de Obrigações de Qualidade (COQL)
  - Gerência de Controle de Obrigações de Universalização e de Ampliação do Acesso (COUN)
  - Gerência de Controle de Obrigações Gerais (COGE)

- Superintendência de Competição (SCP): tem como competência temas como, atuar no sentido de assegurar a justa e livre competição no setor de telecomunicações, promover resolução de conflitos, avaliar a estrutura de custos das prestadoras, entre outros.
- Superintendência de Relações com Consumidores (SRC): tem como competência temas como, promover a proteção e defesa dos direitos dos consumidores, fomentar a resolução de conflitos entre prestadoras de serviços de telecomunicações e consumidores, entre outros.
- Superintendência de Fiscalização (SFI): tem como competência temas como, fiscalizar a execução, a comercialização e o uso dos serviços de telecomunicações, inclusive dos Serviços de Radiodifusão sonora e de sons e imagens em seus aspectos técnicos, supervisionar as gerências regionais, entre outros.
- Superintendência de Administração e Finanças (SAF): tem como competência temas como, realizar a gestão administrativa, orçamentária, financeira e contábil da Agência, gerir o desenvolvimento de talentos, entre outros.
- Superintendência de Gestão Interna da Informação (SGI): tem como competência temas como, gerir a infraestrutura de tecnologia da informação, redes, serviços e sistemas de informação e comunicação, necessários ao desempenho das atividades institucionais da Agência, manter a política de segurança da informação, entre outros.

Cada estado possui uma entidade, seja ela uma Gerência Regional ou uma Unidade Operacional. Com exceção da Unidade Operacional de Brasília, que é vinculada diretamente à sede, cada Unidade Operacional está vinculada diretamente a uma Gerência Regional. Ao todo são 11 GR’s e 16 Unidades Operacionais.

O mapa estratégico da Anatel, previsto no Plano Estratégico, é a representação visual dos objetivos que vão impulsionar a atuação da Agência nos próximos dez anos. Esses objetivos estão subdivididos em quatro perspectivas: Financeira, Pessoas e Conhecimento, Processos e Resultados. A perspectiva de Resultados contempla os objetivos finais da Anatel, entendidos como aqueles que visam a entrega de um serviço diretamente à sociedade. Um dos objetivos dessa perspectiva é promover a ampliação do acesso e o uso dos serviços, com qualidade e preços adequados.

Nesse sentido, a Agência tem trabalhado para a ampliação das redes de acesso aos principais serviços de interesse coletivo (telefonia fixa, telefonia móvel, banda larga e TV por assinatura), a promoção do uso desses serviços, o atingimento de um patamar de excelência na qualidade de prestação e o estabelecimento de preços compatíveis com as diversas realidades econômico-financeiras, tanto dos potenciais consumidores como das empresas prestadoras. Além disso, busca um cenário em que todo e qualquer brasileiro, independentemente de classe ou localização geográfica, possa estar efetivamente integrado a essa nova sociedade da informação, aproveitando-se, de forma isonômica, de todos os benefícios inerentes ao acesso aos meios de telecomunicação.

A perspectiva de Processos abrange os objetivos relacionados aos processos-chave da Anatel, aos pontos críticos que deverão ser aperfeiçoados para viabilizar maior agregação de valor aos objetivos da perspectiva de Resultados.

Dentre as perspectivas de processos está a promoção da melhoria do desempenho da prestação dos serviços de telecomunicações. Entende-se por promover a melhoria do desempenho da prestação dos serviços de telecomunicações, a aderência entre as obrigações impostas às prestadoras de serviços de telecomunicações pela Anatel e o cumprimento destas pelas prestadoras.

Dentro de um contexto histórico, e com o intuito de atender as obrigações decorrentes dos Compromissos assumidos com a FIFA em 2007, a Anatel criou um Grupo de Trabalho o qual contava com a participação de diversas áreas da Agência, criou-se no âmbito da Anatel o “Projeto Setor”, que visava garantir a construção, por parte das prestadoras de telecomunicações, de uma infraestrutura de alto desempenho compatível com as necessidades de comunicações que demandavam alto tráfego de dados e voz, qualidade e acesso a todos os usuários dos principais serviços outorgados. O Projeto Setor foi composto por diversos subprojetos, dentre

os quais se encontrava o Projeto de Segurança de Infraestruturas Críticas de Telecomunicações.

O Projeto de Segurança de Infraestruturas Críticas de Telecomunicações, denominado na Agência de SIEC tinha como necessidades corporativas, a identificação e a avaliação dos riscos que poderia afetar a segurança das redes de infraestruturas críticas de telecomunicações no País e que, de algum modo, prejudicar a qualidade destes serviços. Preveria ainda no Projeto a realização do monitoramento de todos os elementos das redes de telecomunicações, com foco inicial nos Grandes Eventos Internacionais.

Pretendeu-se, que o processo para gestão de riscos a ser usado pela Anatel estivesse em consonância com a Norma ABNT NBR ISO 31000:2009 – Gestão de Riscos – Princípios e diretrizes. Ademais, o processo para gestão de riscos e monitoramento de redes de telecomunicações também deveria incorporar uma Regulamentação que tratasse da Gestão de Riscos do Setor de Telecomunicações.

Assim, almejou-se a introdução de um ambiente preventivo para o controle da qualidade e dos investimentos em rede de telecom, melhorando a percepção do usuário dos serviços, de forma a atuar proativamente, antecipando possibilidades de interrupções e de má prestação dos serviços.

Para a implementação do processo de gestão de riscos e monitoramento de redes de telecomunicações, seria necessário o tratamento de grande quantidade de dados obtidos das prestadoras de serviços de telecomunicações e das fiscalizações realizadas pela Anatel. Deste modo, seria necessária a disponibilização de uma solução de tecnologia da informação que operacionalize essas funcionalidades, no intuito de minerar tais informações, bem como uma infraestrutura robusta que pudesse dar o suporte necessário à solução.

O primeiro passo da implantação da solução foi elaboração de um inventário dos ativos que terão seus riscos analisados. Devido à enorme quantidade de ativos de telecomunicações existentes no país, fez-se necessário a priorização dos ativos mais relevantes ou estratégicos, que serão objeto da gestão de riscos. Estimou-se que o número de ativos estratégicos era em torno de 5.000 (cinco mil). Os ativos que deram suporte aos grandes eventos esportivos internacionais fizeram parte deste rol.

O monitoramento das redes de telecomunicações destina-se a permitir que o regulador obtenha informações periodicamente do estado das redes, bem como formar um histórico das condições das redes. O módulo de redes da solução está

integrado com os módulos de gestão de risco de forma a permitir a troca de dados sobre os eventos relevantes ocorridos nas redes que possam influenciar no nível de risco das redes e serviços de telecomunicações.

O Projeto para aquisição de uma solução capaz de avaliar os riscos das infraestruturas críticas das redes de telecomunicações brasileiras foi previsto no Plano Diretor de Tecnologia da Informação – PDTI 2012/2014 da Anatel, no subitem 22.3.9.6, sob o qual o projeto de segurança da infraestrutura crítica está denominado, constando do item 22.3.9.6.1.

Neste contexto, pretende-se avaliar as possíveis incertezas no processo de verificações e análise dos riscos das redes de telecomunicações baseadas na análise da solução adquirida pela Anatel.

Dessa forma, este projeto de pesquisa visa apresentar uma das formas em que o uso da solução adquirida pela Anatel pode contribuir para a avaliação das Redes de Telecomunicações Brasileiras, em especial às Redes de Cabos Submarinos que atendem as saídas de tráfego internacional, em especial no estabelecimento do contexto de riscos referente à paralisação ou degradação desse serviço.

Figura 13 Contexto Externo.

Resumidamente, dentro do Contexto Interno, a Gerência de Controle de Obrigações de Qualidade, vinculada à Superintendência de Controle de Obrigações da Anatel, é a área responsável para avaliar e gerenciar a ferramenta de **Governança, Riscos e Conformidade (GRC) e monitoração de Redes,** adquirida por meio de Pregão Eletrônico no ano de 2012, o qual pode mensurar os riscos relativos à eventual mau funcionamento das Redes ópticas submarinas;

3.3. CONTEXTO DE AVALIAÇÃO DE RISCOS

3.3.1. Definição de contexto

Quando da decisão da implementação de uma gerência de riscos, faz-se extremamente necessário o estabelecimento de um contexto bem definido, que serão os parâmetros básicos para que possa ser diagnosticado com excelência o escopo dos riscos que serão considerados.

Conforme exposto em AS-NZS (2004), esse contexto além de detalhar o ambiente interno e externo da organização, se estende a definir o propósito da aplicação da gerência de riscos de segurança da informação, o seu ambiente, seus objetivos, suas estratégias, os critérios utilizados em cada um dos processos que a compõem e a elaboração de uma estrutura lógica de seguimento para o restante do processo de gestão.

A atividade de apreciação de riscos se divide em análise de riscos e avaliação de riscos, que são descritas a seguir:

3.3.2. Análise de Riscos

A análise de riscos se subdivide em identificação de riscos e estimativa de riscos, que são descritas a seguir.

Identificação de riscos

Identificar os riscos é delinear e caracterizar os eventos que podem interferir nos propósitos de uma atividade, projeto, processo, organização etc., a fim de gerenciá-los. Para isso, como exposto em IRM (2002), é necessário um conhecimento intrínseco da organização, do campo em que ela atua, do ambiente em que ela existe, das relações e serviços jurídicos, políticos, sociais, culturais que ela engloba, e sobretudo ter uma visão ampla de seus objetivos, descrevendo as informações críticas para o seu sucesso.

o Pode-se dividir a identificação de riscos nas seguintes etapas: identificação dos ativos, identificação das vulnerabilidades, identificação das ameaças, identificação das consequências, identificação dos controles existentes e registro dessas informações.

3.3.2.1. Estimativa de riscos

Esse processo tem por objetivo desenvolver a compreensão dos riscos. A observação nessa etapa se baseia nas consequências de um determinado evento e nas suas probabilidades de acontecer.

Analisando a natureza, as consequências e as probabilidades dos mesmos, decide-se se os riscos devem ser tratados, com qual prioridade e quais as estratégias de tratamento apropriadas e com melhor custo-benefício relativos aos tais riscos.

A estimativa de riscos, segundo AS-NZS (2004), pode ser qualitativa (geralmente a primeira a ser feita, dando uma visão geral dos níveis dos riscos e identificando os riscos de maior prioridade), quantitativa (em geral utilizada depois de uma estimativa qualitativa, atuando sobre os riscos mais prioritários, ou que podem trazer maior impacto por meio de suas consequências) ou semi-quantitativa.

3.3.2.2. Avaliação de riscos

De acordo com IRM (2002), o processo de avaliação de riscos consiste na comparação dos riscos estimados com os critérios que foram estabelecidos no processo de definição do contexto, que envolviam custos associados ao tratamento dos riscos, benefícios, fatores ambientais, opiniões das partes interessadas etc. Além de considerar a definição do contexto, deve-se levar em conta outros documentos e requisitos tais como: requisitos contratuais, requisitos legais e requisitos regulatórios.

Conforme explicitado em ABNT (2008), o principal objetivo desse processo é a tomada de decisões a respeito dos riscos que necessitam de tratamentos e daqueles que necessitam de tratamentos prioritários, baseando-se nos objetivos e no grau de oportunidade que pode ser gerado para a organização, respeitando o contexto definido.

3.3.2.3. Tratamento de riscos

No processo de tratamento de riscos, de acordo com AS-NZS (2004), identificam-se opções para proteger a organização dos riscos identificados, analisados e avaliados.

Avaliam-se esses tratamentos decidindo-se quais opções serão adotadas e em qual ordem serão executadas, fazendo-se a preparação para que seja possível executá-las e finalmente, implementando as ações planejadas.

Fazer com que uma organização não fique exposta a nenhum risco é impossível. Diante dessa certeza, faz-se extremamente necessário a definição de prioridades e de direções dos esforços e controles a fim de minimizar o impacto negativo e maximizar as oportunidades.

Consoante ao definido em ABNT (2008), o processo de tratamento de riscos pode ser de quatro tipos, não excludentes entre si: redução do risco (seleção de

controles apropriados para mitigar os riscos de segurança da informação), retenção do risco (que refere-se à opção de não implementar controles para tratamento de um risco, diante do fato de o nível desse risco atender aos critérios para a aceitação de riscos), evitar o risco (eliminação das atividades/eventos que causam o risco ou alteração nas condições de operação de tais) e transferência do risco (compartilhar determinados riscos com entidades externas, para que o mesmo seja tratado de forma mais eficaz).

Aceitação do risco de segurança da informação

De acordo com ABNT (2008), é nessa atividade que se delimita quais riscos serão ou não aceitos formalmente, de acordo com os critérios para aceitação de riscos, descrevendo como seu tratamento se dará, os possíveis riscos residuais resultantes e as condições associadas a essas decisões.

3.3.2.4. Monitoramento e revisão

O processo de monitoramento e revisão ao longo do gerenciamento de riscos e ao seu final assegura que novos riscos que surjam durante a execução do projeto/atividade não sejam desconsiderados ou que mudanças nos riscos serão rapidamente reconhecidas pelo fato de os mesmos serem analisados e revisados frequentemente, além de revisar a execução de respostas a riscos enquanto avalia sua eficácia. Em suma, esse processo prima pela continuidade da pertinência da gerência de riscos, conforme entendimento explícito em AS-NZS (2004) e em ABNT (2008).

3.3.2.5. Comunicação e consulta

Esse processo engloba os diálogos com as partes interessadas, internas e externas, sabendo que os mesmos têm visões pertinentes acerca dos riscos da organização e que essas percepções têm grande influência em quais decisões são tomadas. Então, partindo dessa premissa, as comunicações e consultas a esses intervenientes devem ser constantes, envolvendo assuntos tanto dos riscos, quanto da sua gestão ao longo de todo esse macroprocesso que é a gestão de riscos.

Além disso, quando existe uma comunicação efetiva, a distribuição de responsabilidades e o entendimento da base em que se tomam as decisões são facilitados.

3.3.3. Problema a ser resolvido na organização

Avaliação do Cenário Atual da Gestão de Riscos nas Redes de Cabos Submarinos Brasileiras após implantação da Ferramenta de Governança, Riscos e Conformidade (GRC) e monitoração de Redes na Agência, com intuito de antecipar-se com ações Proativas para melhor adequação dos Normativos e Regulamentos presentes na Agência que permeiam àquelas Redes para Garantir maior Desempenho, Disponibilidade e Qualidade para os Usuários de Telecomunicações.

3.3.4. Descrição do problema a ser resolvido.

À época a Anatel não avaliava, de forma sistemática, o risco de segurança associado às infraestruturas críticas de telecomunicações, nem obtinha as informações periódicas do estado de todos os elementos das redes das prestadoras de telecomunicações. Além do mais, não havia normas dentro da Agência que estabelecem requisitos para o gerenciamento dos riscos relacionados à segurança das infraestruturas críticas e ao monitoramento das redes de telecomunicações. Portanto, era necessária a ação da Agência no sentido de identificar e minimizar riscos, e monitorar as redes de telecomunicações brasileiras.

Destaca-se que o tema de Infraestrutura Crítica foi amplamente discutido ao longo desses últimos 10 (dez) anos. Na Anatel, a Portaria nº 222, de 12 de março de 2007, criou Grupo de Trabalho para tratar deste tema, em função do projeto de Proteção de Infraestrutura Crítica de Telecomunicações (PICT), que foi executado pela Fundação CPqD, no período de 2007 até 2009, com recursos do Fundo para o Desenvolvimento Tecnológico das Telecomunicações (Funttel).

O projeto PICT foi formalizado por meio do Convênio MC nº 007/2005, e seus aditivos, celebrado entre a União, por intermédio do Ministério das Comunicações e a Fundação CPqD. Dentre os principais resultados obtidos pelo projeto PICT, destacam-se:

- Identificação da Infraestrutura Crítica de Telecomunicações no escopo dos jogos Pan-Americanos de 2007. Os resultados obtidos subsidiaram o planejamento da segurança da infraestrutura de telecomunicações utilizado durante os XV Jogos Pan-americanos;
- Contextualização sobre o tema no mundo. Esse estudo direcionou a estratégia nacional de proteção de infraestrutura crítica e contribuiu para o fomento da criação de grupos de trabalho na esfera do governo federal;

- Desenvolvimento do sistema de proteção de infraestrutura crítica de telecomunicações.

Desta forma, o tema Segurança de Infraestruturas Críticas nas Telecomunicações tem sido amplamente discutido em âmbito nacional e internacional. Porém, a Anatel, até o primeiro semestre de 2013 não possuía uma estrutura interna para gerenciar os riscos associados às redes e serviços de telecomunicações. Portanto, mostrava-se necessária a atuação da Anatel neste campo, evidenciado pela necessidade dos Grandes Eventos Internacionais ocorridos no País, quando eventuais ataques às redes se tornam mais propensos e a administração de riscos passa a ser imperativa. Destaca-se também a necessidade de manutenção sistemática da qualidade dos serviços das redes de telecomunicações brasileiras.

Além disso, era extremamente necessário o monitoramento das redes de telecomunicações, para permitir que a Anatel obtivesse periodicamente informações do estado de todos os elementos das redes, bem como para formar um histórico das condições das redes. Era necessária uma solução que abarcasse a verificação dos estados das redes de telecomunicações bem como a gestão de riscos associadas à operacionalização daquelas redes.

Pela quantidade de elementos na estrutura das redes de telecom no Brasil, foi definido que todos os elementos de redes seriam monitorados, porém somente os elementos considerados críticos seriam objeto da Gestão de Riscos.

A proposta permitiu desenvolver uma modelagem de risco à segurança de infraestruturas críticas e de monitoramento de redes para o mercado de telecomunicações, incluindo serviços; obter uma solução de suporte às atividades de gestão de risco e de monitoramento de redes relacionadas à segurança das infraestruturas críticas de telecomunicações, configurando-a para as necessidades do regulador de telecomunicações em conformidade com a Norma ABNT NBR ISO 31000:2009 de Gestão de Riscos, em que os dados a serem utilizados devem ser obtidos nas bases da Agência e dos Centros de Gerência de Rede das prestadoras de serviços de telecomunicações.

A Solução deveria integrar com as bases de dados disponíveis nos sistemas da ANATEL, como por exemplo, SDSAC, STEL, RADAR, SICI e RGQ, coletar dados de sistemas externos, processar informações desejáveis e criar como saída um mapeamento de risco e do monitoramento das redes e serviços de telecomunicações

com informações georeferenciadas das estações e centrais que formam as redes de telecomunicações.

3.4. OBJETIVO GERAL

Considerando o cenário atual, o que se pretende propor com esse trabalho é averiguar a existência de legislação no País que possam garantir a proteção das infraestruturas das redes de cabos submarinos no trecho das águas sob jurisdição brasileira e em sua rota terrestre. Pretende-se ainda avaliar o atual processo de gerenciamento de segurança das infraestruturas críticas das redes de telecomunicações no tocante às saídas de dados internacionais por meio de cabos submarinos.

3.5. OBJETIVO ESPECÍFICO

- Estudo das Infraestruturas Críticas das Redes de Cabos Ópticos Submarinos no País para construir a base conceitual para a continuidade eficiente do trabalho;
- Realizar estudo de dimensionamento do tráfego de dados atuais e projeção de crescimento no que se refere às saídas de dados internacionais providas por meios cabos ópticos;
- Estudar a viabilidade de criação de uma regulamentação específica para proteção da malha de cabos submarinos que permeiam a costa brasileira ou que estão instalados no território nacional, que abranja também a segurança física dessas instalações;
- Recomendar o monitoramento, por meio de Painéis (Dashboards), no âmbito da Agência, das redes de cabos submarinos no Brasil com intuito de avaliar seu crescimento e desempenho;
- Discussão dos resultados obtidos.

3.6. ESCOPO E CONTEXTO

Um processo de gestão de riscos de segurança da informação (GRSI) caracteriza-se como um dos elementos mais importantes para sua efetividade, visto que o mesmo permite a identificação das necessidades e prioridades de segurança

da informação da organização com base em análises e avaliações que se guiam pelos critérios e requisitos definidos pela própria organização. Segundo [ABNT 2008b], administrar os riscos de segurança da informação aos quais se está sujeito contribui de maneira significativa para o sucesso da organização e de seus negócios.

3.7. SITUAÇÃO PROBLEMA

Com o crescimento exponencial do volume de dados trafegados entre o Brasil e os outros países a exposição de determinadas infraestruturas das redes de telecomunicações, em especial das redes de cabos submarinos, gera vulnerabilidade à segurança da informação nesse segmento.

Antes de propriamente adentrar no estabelecimento do contexto buscou-se após o mapeamento do processo mapear por técnica de brainstorm com 15 especialistas da Anatel de diversas áreas (SCO, ATC, SPR, SOR, SRC, SFI, SCP), possíveis incertezas para esse processo. Dessa forma, foram consolidadas 5 (cinco) opiniões de cada especialista coletada por meio de post-it, totalizando 78 incertezas que posteriormente por meio de um debate orientado foram agrupados em grandes grupos e consolidados nas seis grandes incertezas abaixo para o atendimento processo:

Quais seriam os potenciais benefícios da proteção das redes de cabos submarinos para o País? Quais as formas eficientes de garantir essa proteção? Tal preocupação é viável?

Quem é responsável pela segurança das infraestruturas críticas de Telecomunicações do Brasil?

A Agência Nacional de Telecomunicações – ANATEL possui formas de mensurar a qualidade da prestação dos serviços das redes de telecomunicações que trafegam por meio de cabos submarinos no Brasil?

É dever da Agência Nacional de Telecomunicações – ANATEL, garantir a segurança das infraestruturas críticas de telecomunicações no País?

Quais as principais vulnerabilidades existentes nas redes de Cabos Submarinos nas telecomunicações Brasileiras?

Em caso de crises o Brasil consegue garantir a operação mínima dessas redes de Telecomunicações, digam-se Redes de Cabos Submarinos?

Quais os eventos críticos no setor de telecomunicações ocorridos no Brasil nos últimos anos?

Pergunta Chave:

Considerando uma abordagem da gestão da segurança da informação voltada à Riscos, em especial com o enfoque na proteção das infraestruturas críticas de telecomunicações no País, é possível utilizar as técnicas de avaliação de riscos FMEA, ETA e FTA para avaliar as falhas das redes de Cabos Submarinos Brasileiras, em especial aplicar seu uso com auxílio da Solução de Software de Governança, Riscos, Conformidade (GRC) e Monitoramento das Redes de Telecomunicações Brasileiras, adquirida pela Agência Nacional de Telecomunicações, pode Garantir maior Desempenho, Disponibilidade e Qualidade para os Usuários de Telecomunicações.

3.8. INFRAESTRUTURAS CRITICAS

Fernandes e Rodrigues (2013) apresentam os conceitos da cibernética, da teoria dos sistemas e das redes complexas; os processos de trabalho, normas e riscos concomitantemente criados no interior das organizações humanas; o impacto da introdução das tecnologias de informação e comunicação nos processos de trabalho das organizações humanas; o surgimento das infraestruturas críticas e a necessidade de sua proteção, segurança e defesa; a abordagem de engenharia de segurança; os fenômenos do *hacking* e do *cracking*; as características do crime organizado na Internet; a ocorrência dos incidentes de segurança que pode conduzir às crises organizacionais; e, por fim, o sistema normativo de Gestão de SIC em desenvolvimento no país.

Fernandes e Rodrigues (2013) propõem uma pesquisa de estudo de caso na investigação da aplicação do processo de trabalho racional na gestão de SIC das organizações públicas federais do Brasil.

Argumentam ainda que a Segurança da Informação e Comunicações - SIC, desenvolvida na Administração Pública Federal brasileira, considera a natureza complexa e distribuída dos órgãos e instituições federais, muitos deles com estruturas geograficamente distribuídas no território nacional, e cujas ações são pautadas pela transparência e intensa relação com a sociedade.

A Segurança da Informação, definida como a “proteção dos ativos de informação de uma organização contra um grande número de ameaças, visando assegurar ou garantir a continuidade das atividades de negócio ou o cumprimento da

missão crítica desta organização, minimizando os riscos às suas atividades, maximizando retorno sobre seus investimentos e as oportunidades de sucesso".

De forma bastante simplificada, infraestruturas críticas são artefatos tecnológicos fundamentais usados por um sistema viável, ou dos quais ele depende.

CAPÍTULO 4

4. FUNDAMENTAÇÃO CONCEITUAL

4.1. CABOS SUBMARINOS

O Cabo submarino é um cabo telefônico especial, que recebe uma proteção mecânica adicional, própria para instalação sob a água, por exemplo, em rios, baías e oceanos. Normalmente dispõe de malha de aço e de um isolamento e proteção mecânica especial. Este tipo de cabo telefônico é utilizado principalmente em redes internacionais de telecomunicações, que interligam países e continentes. No Brasil, pelo seu tamanho continental, o cabo submarino é utilizado para interconectar toda a sua costa. Seu tipo pode ser metálico, coaxial ou óptico, sendo este último o mais utilizado atualmente.

A composição de uma estação de cabos submarinos, independentemente da empresa proprietária, possui, fundamentalmente, os mesmos tipos de equipamentos: Terminais de Linha Submarinos (SLTE), DWDM para uso metropolitano/terrestre, equipamentos de cross-connections, roteadores para atendimento a clientes e DCN (Data Communications Network), estações de trabalho de sistemas de gerência, sistemas de ar-condicionado, energia DC (retificados e baterias) e energia AC (geradores, UPS).

O Sistema de Comunicação de Longa Distância utilizando Cabos Submarinos está representado na figura abaixo:

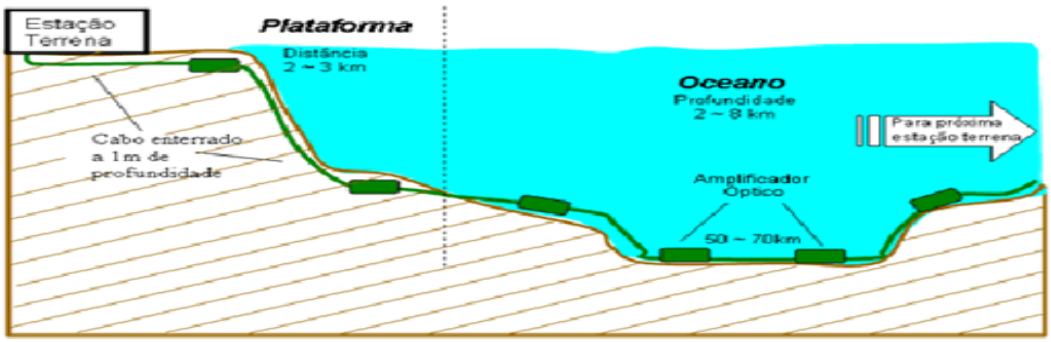


Figura 14 Cabo Submarino

Na Estação Terrena estão os equipamentos responsáveis pela regeneração do sinal óptico e pela demultiplexação dos sinais separando-os em canais e posteriormente disponibilizando-os para a distribuição aos usuários finais. É na Estação Terrena que o cabo submarino chega quando entra no continente. Além da Estação Terrena, os sistemas submarinos completam-se com os Pontos de Presença (POP). Tanto a Estação Terrena como os POPs são dotados de sistemas de energia e segurança com redundância de 100% incluindo a entrada de energia da concessionária, geradores, sistema ininterrupto de energia (no-break) e ar-condicionado. Os sistemas de prevenção, proteção e combate a incêndio também são itens cuidadosamente estudados e implementados. O centro de gerência do sistema (NOC – Network Operation Center) geralmente é construído em uma Estação Terrena ou POP. Através de alarmes e sistemas de monitoração, o NOC permite o controle de tráfego, a vigilância dos sinais, identificação de problemas e a manutenção do sistema, 24 horas por dia, 7 dias na semana.

A principal característica dos sistemas de comunicações de cabos ópticos submarinos, além da sua alta capacidade de transmissão é a distância que se pode atingir, chegando a até 9.000 km sem necessidade de regeneração do sinal. Nos sistemas que utilizam fibras ópticas de terceira geração consegue-se atingir espaçamentos de até 60km entre repetidores. Já nos sistemas que utilizam cabos com fibras óticas de quarta geração, estes espaçamentos podem atingir até 100Km.

Além disso, o cabo óptico, amplificadores e regeneradores utilizados em sistemas submarinos são projetados para resistirem à pressão de água de até 8.000m de profundidade (pressão igual a 800 atmosferas). A estrutura dos

componentes, incluindo os componentes ópticos, é de altíssima confiabilidade, normalmente assegurando 25 anos de vida útil.

Os sistemas submarinos atuais têm capacidade de transmitir vários sinais ópticos independentes, cada um com um comprimento de onda característico (lambda). O método pelo qual vários sinais em diferentes comprimentos de onda são combinados numa única fibra é conhecido pelo nome de multiplexação por divisão de onda densa (DWDM). Os DWDM atualmente em funcionamento nos cabos submarinos trabalham com comprimentos de onda com velocidade de transmissão de 2,5Gbps, 10Gbps, 40 Gbps e 100 Gbps. Os equipamentos de DWDM ficam nas Estações Terrenas. Seu projeto, normalmente, permite um crescimento gradual, desde um único comprimento de onda até múltiplos comprimentos, à medida que aumentem as necessidades de capacidade.

O equipamento SDH oferece às redes ópticas funções de multiplexação e proteção. Todas as interfaces são padronizadas de acordo com normas internacionais, permitindo a sua interligação com outras redes submarinas, terrestres e de satélite. Podem estar instalados tanto na Estação Terrena como no POP.

Os amplificadores ópticos compensam as perdas no cabo submarino devidas à atenuação do sinal. São conectados ao cabo a intervalos de distância apropriados e devolvem aos pulsos óticos a sua amplitude original, sem necessidade de ter que convertê-los à sua forma eletrônica nos repetidores submarinos. Eles não realizam a regeneração do sinal, que é feita na Estação Terrena. Os amplificadores ópticos são projetados de modo a poder transportar a capacidade da fibra através dos vários milhares de quilômetros entre as Estações Terrenas. A alimentação dos amplificadores ópticos de um sistema óptico submarino é feita remotamente a partir das Estações Terrenas. A voltagem necessária para a alimentação dos amplificadores gira entre 4.000V a 10.000V/DC.

O cabo submarino, normalmente, acompanha a topografia do fundo do oceano e fica praticamente “estacionado” no leito submarino. Isto se deve ao próprio peso do cabo e ao peso dos amplificadores (em torno de 500 kg cada um). Assim, na parte oceânica o cabo submarino não necessita de uma maior proteção além da utilizada para resistir à pressão de água em grandes profundidades. Podem-se utilizar vários tipos de cabo de acordo com as condições do leito oceânico e as funções da rede. O cabo tronco normalmente possui quatro pares de fibras e os ramais dois. Em águas profundas o tronco e ramais são leves, não havendo a necessidade de uma

blindagem mais pesada. Perto da costa utilizam-se cabos blindados de vários tipos para minimizar as ameaças externas das âncoras das embarcações e barcos pesqueiros. A fibra é desenvolvida especificamente para aplicações submarinas e produzida especialmente para transportar a capacidade da fibra através dos vários milhares de quilômetros entre as Estações Terrenas.

Uma estação de cabos submarinos é, basicamente, uma estação de telecomunicações, cujo meio principal de transmissão é a fibra óptica, de capacidade muito maior do que as de outros meios, tais como transceptores em micro-ondas, pares metálicos, satélites, etc.

Os cabos submarinos, como o nome indica, são lançados nos oceanos, permanecendo em operação por um tempo de vida útil em redor de 25 anos, limitada pela quantidade de defeitos em seus repetidores – instalados no leito do oceano e que amplificam os sinais a cada intervalo de 50 quilômetros – ou por mudança relevante de tecnologia.

Os equipamentos diretamente conectados aos cabos ópticos submarinos – chamados, genericamente, de SLTE (*Submarine Line Terminal Equipment*) – têm a função de transmitir os sinais de telecomunicações (voz, vídeo, dados) na forma de luz, injetando-os/extraindo-os nas/das fibras ópticas dos cabos submarinos.

Associados aos equipamentos SLTE, existem, também, os chamados equipamentos de *cross-connections* (conexões cruzadas), aos quais conectam-se clientes de várias velocidades ou taxas de transmissão, em 2 Mbps, 155 Mbps, 622 Mbps, 2.5 Gbps e 10 Gbps. Esses equipamentos de cross-connections, em geral, podem-se afirmar, constituem-se nas interfaces entre os clientes e os terminais de linha óptica submarinos (SLTEs). Eles agregam vários clientes de mais baixas taxas de transmissão e formam feixes de 10 Gbps, dirigidos aos SLTEs. Mais recentemente, têm surgido casos de conexão direta de clientes aos SLTEs, na velocidade de 10 Gbps.

Nos casos das estações de cabos submarinos têm-se a elas acesso via sistemas (chamados de backhauls) de repetidores e fibras ópticas terrestres instalados entre as telehouses ou POPs e as citadas estações de cabos submarinos, respectivamente.

Como em outras estações de telecomunicações, as de cabos submarinos são dependentes, em termos de disponibilidade e de confiabilidade, de sistemas de infraestrutura – geralmente compostos por sub-sistemas de ar-condicionado, energia

CA e CC, proteção e combate a incêndio e controle de acesso, DCN (Data Communications Network), Comunicações Internas (PBX, PCs), Equipamentos de Supervisão (Servidores, Estações de Trabalho). Sobre cada um desses sub-sistemas serão fornecidas mais informações nos próximos itens.

4.2. NÚMERO DE FIBRAS ÓPTICAS, CAPACIDADE

Os cabos submarinos instalados entre as estações são equipados com quatro pares de fibras ópticas. Tem-se, em geral, uma ideia errônea de que cabos submarinos de fibras ópticas possuem muitas fibras, em virtude da alta capacidade de transmissão desses cabos. Isso não acontece. Na verdade, são poucas as fibras instaladas. A alta capacidade ainda assim acontece, por conta do que se pode inserir/extrair de tráfego em/de cada fibra. Ao longo do tempo, e dentro de certos limites estabelecidos pela tecnologia, aproveita-se a extrema capacidade de cada fibra apenas instalando mais (ou substituindo antigos por mais novos) equipamentos nas estações de cabos.

Nas estações de cabos submarinos existem bobinas de cabos que funcionam como reserva para os trechos que interligam cada estação ao chamado beach manhole, uma grande caixa localizada na praia, último ponto de acesso ao cabo submarino antes de sua entrada no mar. Falhas neste trecho terrestre são recuperadas com os cabos das citadas bobinas.

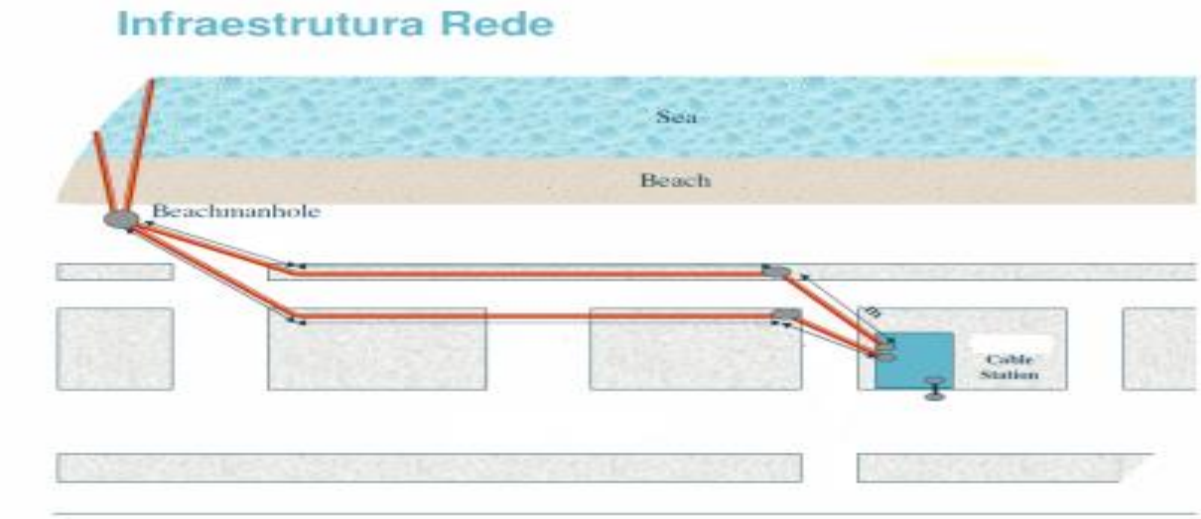


Figura 15 Infraestrutura de Rede

Em caso de falhas em trechos submarinos (defeitos em repetidores ou quebras de cabos), um navio especial é chamado ao local. Este navio já traz consigo,

permanentemente, trechos de cabos submarinos, repetidores e todos os acessórios necessários à recuperação do segmento, incluindo um robô (ROV) responsável por apanhar as pontas de cabos partidos.

4.2.1. SLTEs – Equipamentos Terminais de Linha Óptica Submarinos

Um componente especial que caracteriza uma estação de cabos submarinos é o chamado SLTE. Sua função principal é a de interface com as fibras ópticas submarinas, transmitindo/recebendo a informação agregada de vários clientes em forma de laser.

Existem, nas estações de cabos submarinos, três ou quatro tipos de SLTE instalados, normalmente são fabricados pela Alcatel-Lucent, Infinera, Ciena-Nortel.

Independentemente do fornecedor, esses equipamentos, de maneira geral, executam as mesmas funções através de procedimentos diferentes, de formas mais ou menos compactas, com maior ou menor eficiência, mais ou menos placas envolvidas. Assim, os processos de modulação, demodulação, codificação, decodificação e amplificação são realizados no SLTE através de várias placas – uma por função.

4.3. EQUIPAMENTOS DE CROSS-CONNECTIONS

Os equipamentos de cross-connections têm a função de prover interfaces para a conexão do tráfego de clientes de várias taxas de transmissão às rotas submarinas, que operam em taxas padronizadas de 10 Gbps. Eles, assim, reúnem circuitos de clientes em velocidades tais como 2 Mbps, 155 Mbps, 622 Mbps ..., nos chamados agregados de 10 Gbps, que irão modular portadoras ópticas transmitidas através dos equipamentos SLTE.

Em algumas estações de cabos submarinos na América Latina ainda estão em funcionamento equipamentos de cross-connections instalados pela Lucent no ano de 2001, chamados de BWM (Bandwidth Manager, Gerenciador de Banda).

Após ser submetido a várias atualizações de software, por conta de diversas interrupções de tráfego, o BWM ainda apresenta problemas de corrupção de base de dados, além de, ultimamente, ter apresentado, como era de se esperar após 10 anos de operação, um aumento significativo da taxa de defeito em suas unidades.

Como aconteceu com o SLTE OALW64 da Alcatel, o BWM teve sua linha de produção desativada pela Lucent, isto é, não se fabricam novas

unidades/equipamentos BWM. A Lucent, no entanto, como a Alcatel com o OALW64, tem garantido suporte e manutenção para aqueles equipamentos.

No entanto, nas estações supracitadas na América do Norte, já existe em operação, há algum tempo, um outro modelo de equipamento executando as mesmas funções do BWM, também fabricado pela Lucent, chamado de Lambda United, abreviado para LU. Ele é mais compacto do que o BWM e apresenta menores taxas de defeito em suas unidades. Já existem planos de se substituírem equipamentos BWM por LU em algumas estações do sistema SAC, destinando-se as unidades desativadas do BWM para reservas dos equipamentos que não forem desabilitados.

Equipamentos de DCN

Para que os equipamentos de telecomunicações (SLTE, Cross-Connections) possam ser supervisionados local e remotamente por equipes localizadas nos chamados NOCs (Network Operations Center), existem instalados nas estações de cabos submarinos dispositivos que encaminham comandos e informações de estado entre servidores/estações de trabalho e aqueles equipamentos. Juntos, de maneira global, tais dispositivos constituem a chamada DCN, Data Communications Network (Rede de Comunicação de Dados), entidade que também se constitui de circuitos digitais de conexão entre equipamentos, estações de trabalho (PCs) e servidores instalados nas estações do sistema.

Além da DCN descrita no parágrafo anterior para supervisão de equipamentos de telecomunicações – chamada de DCN EMS (Element Manager System -, existe, também, uma outra DCN utilizada para interconexão dos PBX das várias estações (sistema VoIP), servidores de e-mail, Internet, e de mensagens instantâneas, chamada de DCN Corporativa.

Os dispositivos mais conhecidos das DCNs são os roteadores (em geral fornecidos pela Cisco, Juniper, Huawei), hubs e switches, com fabricantes variados tais como HP e Catalyst. Eles não têm apresentado, após 10 anos de operação, sinais de degradação de desempenho, com pouquíssimos defeitos observados em suas placas.

Tipos de falhas em cabos submarinos

Basicamente, há dois tipos de falhas em cabos submarinos:

‘Shunt fault’, em que o condutor metálico que leva a tensão dos PFEs apresenta fuga para a terra.

Falha total, em que as fibras ópticas são também cortadas.

Tais eventos podem não ser simultâneos.

No Brasil, até 2014 eram quatro, os principais provedores de capacidade de dados que interligam os sites internacionais por meio de cabo submarino. Com intuito de proteger as informações e por se tratar de dados extremamente sensíveis, serão utilizados nomes fictícios das empresas prestadoras do serviço supracitado durante todo o trabalho, a saber: EMPRESA A, EMPRESA B, EMPRESA C e EMPRESA D.

A figura abaixo demonstra a configuração atual da malha de cabos submarinos no Brasil ilustrando as principais saídas internacionais, em especial nas cidades de Fortaleza, Santos, Rio de Janeiro e Florianópolis. Os nomes das empresas foram omitidos da figura.

Figura 16 Rede de Cabos Submarinos no Brasil.

Segundo Natalia Viana (Carta Capital, Dez 2010) um documento disponibilizado pelo Wikileaks mostra que o Departamento de Estado americano pediu que diplomatas em todo o mundo fizessem uma lista da infraestrutura e recursos imprescindíveis aos EUA nos países onde trabalham. No Brasil, a principal

preocupação dos EUA é com cabos de transmissão submarinos em Fortaleza (Alfa e EMPRESA “A”), e com as minas gerenciadas pela britânica Rio Tinto Company e EMPRESA “A” em Minas Gerais e Rio de Janeiro – elas fornecem minério de ferro – e com a Mina Catalão I, em Goiás (explorada pela Anglo American), que fornece nióbio, usado principalmente em ligas de aço. Até a Venezuela tem infraestrutura crítica para os EUA: são os cabos submarinos Alfa da EMPRESA “D” , que passa por Camuri e o da EMPRESA “A”, que passa por Punta Gorda, Catia La Mar, e Manonga.

No que diz respeito às comunicações Internacionais por meio de cabos submarinos, diante desta ameaça, o Brasil, recentemente por meio da Telebrás e a Angola Cable concluiu os estudos do cabo submarino de fibra óptica de seis mil quilômetros que ligará Fortaleza e Luanda, mantendo desta forma uma estrutura de cabos submarinos com uma alternativa de tráfego internacional em caso de haver algum problema com as infraestruturas atuais. A previsão era que as obras de passagem do cabo pudessem começar no ano de 2013 e estivessem prontas até 2014, fato que não ocorreu. A capacidade e custo do projeto serão definidos no edital de licitação internacional para a realização do empreendimento.

A parceria é parte da estratégia da Telebrás de ter uma rede de cabos submarinos ligando o Brasil à África, Europa e Estados Unidos. A empresa trabalha para lançar cinco cabos submarinos – quatro internacionais e um em território brasileiro. Serão 24 mil quilômetros de rede a um custo estimado de R$ 1,8 bilhão.

Em outra vertente, a Alcatel-Lucent e a América Móvil estão construindo conjuntamente o sistema de cabos submarinos América Móvil 1 (AMX-1), com 17.500 km e projetado especificamente para a transmissão de 100 Gbps. O cabo cobrirá a região dos EUA à América Central, chegando ao Brasil e permitirá que a América Móvil ofereça conectividade internacional a todas as suas subsidiárias.

4.4. ATIVIDADE DE ESTUDOS E AVALIAÇÕES DAS REDES

Em meados de maio de 2012, a então Superintendência de Serviços Privados – SPV e a Superintendência de Radiofrequência e Fiscalização - SRF da Anatel realizaram missões com o objetivo de avaliar a infraestrutura de rede de dados que dão suporte as saídas nacionais e internacionais, focando averiguar dentre outros o dimensionamento, tráfego, prospecção de crescimento e planejamento de redes dos principais provedores de Serviço de Comunicação Multimídia - SCM no País.

As referidas missões fizeram parte do conjunto de ações para avaliação do desempenho dos backbones nacionais e internacionais do BRASIL, tendo em vista a rápida demanda por capacidade ocorrida naqueles anos, e dos grandes eventos ocorridos no Brasil como Copa do Mundo e Olimpíadas, dentre outros.

Da atividade de estudos e avaliações das principais redes em operação no Brasil à época, pode-se inferir, conforme dados coletados que:

- EMPRESA “A”:

- Cabo ALFA em desativação.
- Cabo X e Y obsoletos – sem previsão de crescimento
- Falta de investimento
- Falta de manutenção preventiva da rede
- Apenas 2 profissionais trabalhando para gerenciar a rede no Brasil
- Tráfego da Rede acima do limite recomendado 50%
- Não existe gerência proativa.
- Falha de segurança identificada nas dependências da Estação.

- Empresa “B”:

- Rede em expansão
- Manutenção preventiva e corretiva adequado
- Infraestrutura adequada
- Profissionais capacitados
- Falha de segurança identificada nas dependências da Estação.

- Empresa “C”:

- Rede em expansão
- Manutenção preventiva e corretiva adequado
- Infraestrutura adequada
- Profissionais capacitados
- Falha de segurança identificada nas dependências da Estação.

- Empresa “D”:

- Rede em expansão
- Manutenção preventiva e corretiva adequado
- Inexistência de anel redundante na costa oeste da América Latina (Oceano Pacífico).
- Profissionais capacitados
- Falha de segurança identificada nas dependências da Estação.

Principais Riscos avaliados:

- Os pontos críticos de risco das redes de cabo submarinos encontram-se próxima as estações terrestres, beachmanhole e trecho inicial marítimo (20km iniciais).
- No trecho terrestre o risco reside basicamente na possibilidade de rompimento dos cabos por obras, falta de sinalização e falta de manutenção e procedimentos de prevenção de falhas.
- No trecho marítimo, a falta de legislação específica para proteção da área onde os cabos submarinos fazem seu percurso (proteção contra pesca de arrasto).
- As estações de fortaleza encontram-se próximas de áreas de risco.
- Existe concentração dos beachmanhole em regiões muito próximas, o que pode afetar, em casos fortuitos ou de força maior, todas as saídas internacionais das principais saídas.
- Tempo alto de manutenção em caso de rompimento no trecho submarino devido deslocamento do Navio de Manutenção (Europa-Brasil).

4.5. REFERENCIAIS DE INFRAESTRUTURAS CRÍTICAS

Fernandes e Rodrigues (2013a) e Araújo (2013ª) entendem que acerca da complexa infraestrutura de comunicação global em rede propiciada pela Internet, que integra outras tecnologias de informação e comunicações (computadores, software etc) e pessoas, fica claro que vários serviços críticos às sociedades humanas são dependentes da Internet e das TICs.

É sabido que uma parte significativa das infraestruturas críticas do Brasil, assim como em várias nações do mundo, é operada por empresas privadas atuando por concessão pública (CANONGIA, 2010, p. 108). Se há uma ruptura da infraestrutura de TICs que apoia a prestação dos serviços públicos próprios ou prestados sobre o regimento e concessão em qualquer região do mundo, isso também pode gerar graves crises naquela região, inclusive com repercussões extra-regionais (FERNANDES, 2014b).

Veneziano e Fernandes (2010) apresentam diversos conceitos relacionados com a gestão de continuidade de serviços críticos para organizações públicas brasileiras, com base em norma da ABNT (2008). Já Fernandes (2014b), aprofundou a temática e a expandiu para o escopo da proteção das infraestruturas críticas de informação.

Por fim, o trabalho de Vidal e Fernandes (2013) apresenta uma breve visão panorâmica de conceitos associados a controles de segurança física e ambiental, bem como a sistemas de proteção física.

4.6. PREOCUPAÇÕES MUNDIAIS E NO BRASIL

Os documentos apresentados por ex-técnico da CIA Edward Joseph Snowden, acusado de espionagem por vazar informações sigilosas de segurança dos Estados Unidos e revelar em detalhes alguns dos programas de vigilância, evidenciam que a NSA trabalhou para atacar todos os tipos de comunicação, e dão conta de que o principal meio de espionagem usado pela NSA é a internet. Na maior parte do tempo, são utilizados programas que automaticamente coletam e analisam o tráfego da rede. Valendo-se supostamente de “acordos secretos” com companhias de telecomunicações – americanas e britânicas, além de várias outras parceiras de outros países, segundo as denúncias –, a Agência acessa os cabos de comunicação por onde passa o tráfego da rede.

Quando não se estabelece as parcerias, a NSA, segundo consta, age por meio de grampeamento dos cabos submarinos, interceptando comunicações via satélite, atacando dispositivos de rede, tais como routers, interruptores (switches), firewalls, entre outros. A maior parte desses dispositivos sustenta a denúncia, teria capacidade de vigilância já embutidas de fábrica, sendo necessário apenas ativá-las.

Os cabos submarinos podem ser classificados mundialmente como infraestruturas críticas de comunicação, uma vez que cerca de 90% do tráfego de

dados trocados entre os cinco continentes (além de uma boa parte do tráfego de chamadas internacionais) são realizados por meio destes cabos.

O cabo do Sudeste da Ásia, Oriente Médio e Europa Ocidental 4 (SEA-ME-WE 4), que tem um comprimento de 18.800 quilômetros e liga a França, Argélia, Tunísia, Itália, Egito, Sudão, Arábia Saudita, Emirados Árabes Unidos, Paquistão, Sri Lanka, Índia, Bangladesh, Tailândia, Malásia e Cingapura é considerado a espinha dorsal da Internet no Sudeste da Ásia, no subcontinente indiano, no Médio Oriente e na Europa e é um dos cabos mais importantes que foi implantado no fundo do mar, portanto, é considerada uma infraestrutura muito crítica, mesmo com a redundância existente.

De acordo com uma reportagem da revista alemã Spiegel, a Agência de Segurança Nacional dos EUA (NSA, na sigla em inglês) teria conseguido obter informações sobre o gerenciamento da rede do sistema de cabos submarinos – SEA-ME-WE-4 que tem 18 mil quilômetros de extensão, e que em 2005 se tornou o principal meio de conexão para internet e telefonia entre a Ásia e a Europa.

Segundo esta reportagem, o Departamento de Operações Customizadas (Tailored Access Operations) da NSA teria conseguido penetrar no site do consórcio que opera a rede e obter dados sobre a infraestrutura técnica do sistema de cabos. Os especialistas da agência americana estariam de posse de informações sobre uma “parte significativa” do sistema, publicou o semanário em edição de dezembro de 2013.

A grande repercussão dessas denúncias deveu-se tanto pela dimensão tecnológica quanto pela abrangência e importância dos alvos escolhidos para obtenção ilegal de informações. Chamou atenção a falta de cuidado de parcelas dos setores público e privado com informações sensíveis e a forma indiscriminada como a espionagem é feita pelas agências de inteligência dos *Five Eyes.*

De acordo com a análise do Sr. Paulo Sérgio Pagliusi, em depoimento à CPI da espionagem, ocorrida em 2013, conforme relatório final, ainda não se sabe o exato alcance do poderio da Agência de Segurança Nacional (National Security Agency – NSA) americana. Sabe-se apenas que eles estão à frente nas pesquisas sobre criptografia e que lidam com supercomputadores pelo menos dez anos mais avançados do que as tecnologias hoje conhecidas. As instalações da NSA na cidade de Utah contam com um data Center avaliado em US$ 2 bilhões. Ele é capaz de armazenar um iotabyte, medida que comporta toda a informação produzida pelo ser humano nos últimos 500 anos. (BRASIL, 2014).

Mas o cenário de espionagem mundial não é protagonizado somente pela NSA. O monitoramento da rede é uma das ações dos Five Eyes, termo que designa o agrupamento das agências de inteligência de Austrália, Canadá, Estados Unidos, Reino Unido e Nova Zelândia. Essas agências são ligadas por um tratado que autoriza o compartilhamento, entre elas, de informações secretas. O acordo original foi firmado em 1946 entre Estados Unidos e Grã-Bretanha, no contexto da Segunda Guerra Mundial.

Os primeiros países monitorados foram os da extinta União Soviética. Os outros três países foram agregados ao acordo por uma razão técnica: ampliar o nível de vigilância sobre os demais países. Dada a dispersão geográfica dos cinco países, juntos eles conseguem monitorar todos os satélites estacionários no globo terrestre.

De acordo com publicações da imprensa retiradas da Internet os Five Eyes são capazes de monitorar, por exemplo, chamadas telefônicas, de fax, transmissões de internet (fixa ou móvel) e de rádio em todo o mundo. Lidam, também, com inteligência de comunicações, que permite saber quem se comunica com quem, quando e como. Fazem, ainda, análise de tráfego (muito utilizada na área militar) que permite observar um volume de fluxo de informações não usual partindo de determinado órgão.

A receptação de dados compreende inclusive os cabos submarinos, pois essas Agências dispõem de uma tecnologia que permite a interceptação desses cabos mesmo em alto mar (interceptation of vessels). É um fato que surpreende, pois se pensava que isso não mais seria possível com os cabos atuais, feitos de fibra ótica.

De acordo com Cláudia Tozetto[1] “em paralelo ao debate sobre leis que garantam a privacidade dos brasileiros na internet, governo busca reduzir exposição de dados na rede.” As rotas de cabos submarinos que conectam os brasileiros a outros internautas no exterior estão na mira do governo brasileiro após as denúncias de Edward Snowden, ex-técnico de informática da agência nacional de segurança americana (NSA, na sigla em inglês), sobre a espionagem do governo dos Estados Unidos a milhões de telefonemas e e-mails de brasileiros. Atualmente, cerca de 90% do tráfego de dados gerado nas conexões de internet brasileiras passa pelos Estados Unidos, o que torna a maior parte das chamadas de voz, e-mails e bate-papos vulneráveis à interceptação pela NSA.

Como não existem cabos submarinos para ligar todos os países, os pacotes de dados passam por grandes pontos de troca de tráfego (PTTs), data centers onde

redes de grande porte de empresas de internet, provedores e operadoras se encontram. “É como numa rodoviária, onde diversas empresas de ônibus chegam para pegar e deixar passageiros”, compara Demi Getschko, diretor-presidente do Núcleo de Informação e Coordenação do Ponto BR, órgão que implementa as decisões e projetos do Comitê Gestor da Internet no Brasil (CGI).

Os pacotes de dados passam por PTTs de grande porte, como o NAP das Américas localizado em Miami (EUA). Além dele, existem outros 13 PTTs para troca de tráfego internacional no mundo, nenhum deles no Brasil. Nestes data centers, grandes roteadores recebem informações trazidas por cabos submarinos, verificam o destino e redirecionam os pacotes de dados para outros cabos que os levem até seu destino final. “Os EUA são um ponto de concentração, porque recebem muito tráfego e geram muito tráfego de internet”, diz Getschko. “A maior parte do tráfego de dados internacional acaba passando pelos EUA em algum momento.”

Segundo o NIC.br, “antes uma questão apenas de logística, o controle sobre os cabos submarinos que conectam as redes de internet em todo o mundo se tornou questão de segurança nacional. Documentos da NSA sobre o programa de espionagem americano obtidos pelo jornal "O Globo" apontam que a agência utiliza um programa chamado Fairview para coletar dados em redes de comunicação em todo o mundo, por meio de uma parceria com uma grande operadora americana”.

4.7. RESPONSABILIDADES

Uma vez implantada a gestão de risco e de monitoramento das redes e serviços de telecomunicações, a Anatel poderia melhor observar pontos em que há indícios de irregularidades, podendo até auxiliar na priorização das fiscalizações a serem executadas com o intuito de se garantir a qualidade e boa fruição dos serviços.

O Projeto SIEC criava uma nova atividade na Anatel, quer seja uma atividade preventiva de gestão de riscos e uma atividade de monitoramento das redes. Em sendo uma nova atribuição, não existia à ocasião, uma área especifica preparada para gerir e dar continuidade a esta nova atividade.

Na nova atividade de gestão de riscos, introduzida na Agência pelo Projeto SIEC, prevê-se a elaboração de relatórios periódicos relativos à exposição ao risco, com foco na identificação de medidas preventivas para garantir a continuidade do funcionamento das redes de telecomunicações. Além da análise preventiva do cenário de telecomunicações, deveria ser realizado um acompanhamento detalhado

da gestão do risco quando da realização de Grandes Eventos Internacionais, como a Copa das Confederações de 2013 e a Copa do Mundo de 2014. Além dos relatórios periódicos, previu-se um monitoramento constante das condições das redes de telecomunicações.

Abaixo é apresentado diagrama de alto nível da solução contratada pela Anatel:

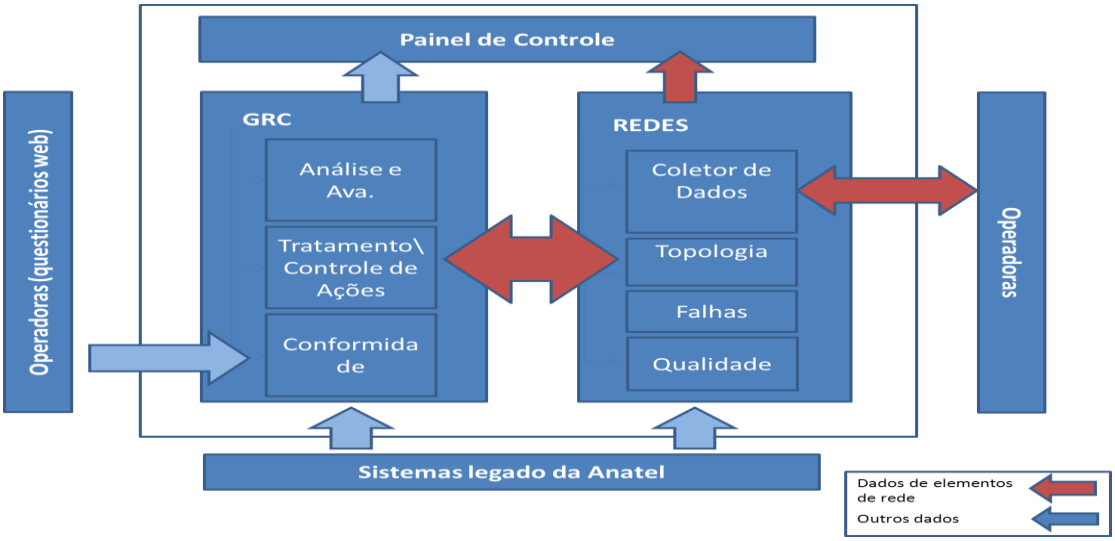


Figura 17 Diagrama SIEC

4.8. FRAMEWORKS E NORMAS IDENTIFICADAS

- ✓ Lei Geral das Telecomunicações – LGT, Lei nº 9.472/1997;
- ✓ Lei de Licitações e Contratos – Lei nº 8.666/1993;
- ✓ Lei sobre pregão – Lei n° 10.520/2002;
- ✓ Instrução Normativa SLTI/MP N° 4 de 12 de novembro de 2010;
- ✓ Norma Brasileira ABNT NBR ISO/IEC 27002:2013 – Técnicas de Segurança - Código de pratica para a gestão da segurança da informação;
- ✓ Norma Brasileira ABNT NBR ISO/IEC 31000:2009 – Gestão de riscos – Princípios e diretrizes;
- ✓ Norma Brasileira ABNT NBR ISO/IEC 31010:2012 – Gestão de riscos – Técnicas para o Processo de Avaliação de Riscos;
- ✓ Norma Brasileira ABNT NBR ISO/IEC 38500:2009 – Governança Corporativa de Tecnologia da Informação.
- ✓ Norma Brasileira ABNT ISO/IEC Guia 73:2009 - Gestão de riscos – Vocabulário;

- ✓ Resolução nº 656, de 17 de agosto de 2015 - Regulamento sobre Gestão de Risco das Redes de Telecomunicações e Uso de Serviços de Telecomunicações em Desastres, Situações de Emergência e Estado de Calamidade Pública;
- ✓ PDTI – Anatel.
- ✓ ITIL (Continuidade de Serviços e Eventos);

4.9. NORMA ISO 31000

4.9.1. Visão geral da Norma

A norma ISO 31000 foi desenvolvida para ser o pilar de sustentação da Gestão de Risco ao apresentar os princípios, estrutura e processo destinados a gestão de risco (ilustrados na figura abaixo). Tais princípios e diretrizes genéricos para a gestão de riscos podem ser aplicados numa ampla gama de atividades das organizações, incluindo estratégias, decisões, operações, processos, funções, projetos, produtos, serviços e ativos, uma vez que todas as atividades de uma organização envolvem risco.

A Internacional Organization for Standardization – ISO (2009) lançou a primeira norma internacional sobre gerenciamento de riscos, conhecida popularmente como ISO 31000, de modo a fornecer princípios e diretrizes genéricas para as organizações relativos ao tema gestão de riscos com aplicação em diversos processos e projetos, e para qualquer tipo de risco, independentemente de sua natureza, sejam positivos (oportunidades) ou negativos (ameaças).

No Brasil, a Associação Brasileira de Normas Técnicas – ABNT incorporou esta norma estrangeira e lançou a ABNT NBR ISO 31000 (2009) que vem sendo adotada desde então, como padrão referencial.

O desempenho e sucesso da aplicação desta norma na organização dependem, entre outros, da eficácia da estrutura de gestão organizacional que servirá de base para diretrizes e princípios.

A norma apresenta como fatores preponderantes para este sucesso o alinhamento da Gestão de Riscos por meio do atendimento a Princípios, que deverão permear toda a Estrutura e resultar na implementação de todo um Processo de gestão, conforme figura abaixo (ABNT, 2009).

Figura 18 Processo de Gestão de Risco.

4.9.2. Ferramentas e Mecanismos para a Gestão de Risco ISO 31010

A norma ISO 31010 versa sobre a gestão de risco, em especial com relação as ferramentas e técnicas que podem ser apropriadas em diferentes contextos.

O processo de avaliação de riscos possibilita um entendimento dos riscos, suas causas, consequências e probabilidade. Isso proporciona uma entrada para decisões sobre a realização de uma atividade; maximização de oportunidades; se os riscos necessitam ser tratados; a escolha entre opções de riscos; a priorização de opções de tratamento de riscos; a seleção mais apropriada de estratégias de tratamento de riscos que trará riscos adversos a um nível tolerável.

Dessa forma é necessário identificar as técnicas mais adequadas ao contexto que se vai trabalhar. Conforme a tabela abaixo se pode verificar de acordo com o nível de informação que se possui.

De acordo com a ISO 31010, existem 31 tipos de técnicas adequadas á análise do risco. Na tabela 2, são apresentadas essas técnicas e a sua classificação quanto ao seu tipo de resultados produzidos; qualitativo (quando se define probabilidade de alto, médio ou baixo risco), semi-quantitativo (quando se combinam várias escalas numéricas para dar origem a um nível de risco baseado numa fórmula de cálculo), ou quantitativo (quando se estimam valores práticos para as consequências e probabilidades, e se produzem valores do nível de risco em unidades específicas definidas no desenvolvimento do contexto).

Tipo das técnicas de análise do risco
Brainstorming
Entrevistas Estruturadas ou Semi-Estruturadas

Técnica Delphi
Listas de Verificação
Análise Preliminar de Risco (PHA)
Estudo da operabilidade e riscos (HAZOP)
Análise de perigos e pontos críticos de controle (HACCP)
Avaliação da toxicidade
Análise “What-if” (SWIFT)
Análise de Cenários
Análise de impacto (BIA)
Análise de causa raiz (RCA)
Análise de modos de falha e efeitos (FMEA)
Modo de falha, efeitos e análise de criticidade (FMECA)
Análise da árvore de falhas (FTA)
Análise da árvore de eventos (ETA)
Análise Causa - Consequência
Análise Causa-Efeito
Análise de Camadas de proteção (LOPA)
Análise da árvore de decisão
Análise da fiabilidade humana
Análise da Gravata Borboleta
Manutenção centrada em fiabilidade
Análise Sneak (SA) e análise de circuitos (SCI)
Análise das Cadeias de Markov
Simulação Monte Carlo
Estatística Bayesiana
Curvas FN
Índices de Risco
Matriz de Risco
Análise Custo/Beneficio
Análise de decisão Multi-Critérios

Quadro 2 Técnicas de análise de risco

4.10. DO PLANO DE GESTÃO DE RISCOS NA ANATEL

O Regulamento de Gestão de Riscos da Anatel tem por objetivo estabelecer definições, procedimentos e condutas para a promoção da disponibilidade, da segurança e do desempenho das redes e serviços de telecomunicações de interesse coletivo, em especial quando da ocorrência de desastres e emergências, ou sua iminência, mediante:

I - Adoção de medidas para acompanhamento do desempenho das redes;

II - Adoção de processo de gestão de riscos das infraestruturas críticas de telecomunicações; e,

III - estabelecimento de medidas de preparação e de resposta para desastre, situação de emergência ou estado de calamidade pública.

O Plano é estruturado conforme os principais artigos da Resolução nº 656, abaixo relacionados:

Art. 5º As prestadoras abrangidas por este Regulamento devem implantar o Plano de Gestão de Riscos – PGRiscos para gerir os riscos que possam afetar a segurança das Infraestruturas Críticas de Telecomunicações.

§ 1º Os riscos citados no **caput** são aqueles relacionados à segurança física e à segurança da informação das Infraestruturas Críticas de Telecomunicações que possam prejudicar a prestação de um serviço de telecomunicações.

§ 2º O Plano de que trata o **caput** deve ser compatível com a base de clientes, a natureza e a complexidade dos produtos, serviços, atividades, processos e sistemas da prestadora.

Art. 6º O PGRiscos das redes e serviços de telecomunicações deve conter, no mínimo:

I - a metodologia utilizada para sua elaboração;

II - a identificação das vulnerabilidades das Infraestruturas Críticas de Telecomunicações e dos riscos associados à continuidade dos serviços de telecomunicações;

III - as medidas adotadas para mitigação das vulnerabilidades mapeadas, incluindo a descrição sobre a redundância física e lógica da rede de transporte e de sinalização, dos principais elementos de redes, como também deve ser incluída uma descrição dos sistemas alternativos de energia;

IV - a hierarquia das Infraestruturas Críticas de Telecomunicações;

V - a estrutura da equipe responsável pelo PGRiscos, contendo a identificação dos responsáveis ou gerência competente;

VI - o Plano de Restabelecimento de Serviços, contendo a identificação de responsável pela execução do plano em cada Unidade Federativa da Área de Prestação de Serviço;

VII - o plano de divulgação interna; e,

VIII - a identificação, se for o caso, da adoção de padrões e normas nacionais ou internacionais quanto à gestão de risco de suas redes.

§ 1º O PGRiscos deve ser aprovado pela diretoria das prestadoras e atualizado ou revisado com a periodicidade adequada.

§ 2º O Plano de Restabelecimento de Serviço deve ser submetido a testes ou simulações para avaliação dos sistemas de controle de riscos, cujos resultados devem constar em relatórios.

§ 3º O PGRiscos deve ser disseminado aos profissionais afetos da prestadora e aos colaboradores terceirizados, em seus diversos níveis, estabelecendo papéis e responsabilidades, resguardando-se o compartilhamento das informações sensíveis apenas para as pessoas que exerçam diretamente atividades de planejamento e execução do Plano, no que couber.

§ 4º Os documentos do PGRiscos e os relatórios mencionados no § 2º, bem como os documentos que comprovem a sua aprovação, deverão estar disponíveis para a Anatel sempre que solicitados.

Art. 7º A estrutura operacional das prestadoras para a gestão das redes e serviços de telecomunicações deve estar capacitada a identificar, monitorar, analisar, avaliar e tratar os riscos.

Paragrafo único. Caso a estrutura de gestão de risco seja única para o Grupo Econômico, deve ser identificada a prestadora responsável por cada função.

CAPITULO 5

5.METODOLOGIA

Após a implementação da ferramenta SIEC – Sistema de Infraestrutura Criticas das Redes de Telecomunicações na Anatel, a pesquisa realizada identificou que, em Relação às Redes de Telecomunicações, apesar de existirem dados e indicadores

específicos para avaliação de Riscos , e o Regulamento sobre gestão de risco das redes de telecomunicações contempla previsões de obrigações da estrutura operacional das prestadoras para a gestão das redes e serviços de telecomunicações, que deve estar capacitada a identificar, monitorar, analisar, avaliar e tratar os riscos. Atualmente a área de controle de obrigações de qualidade da ANATEL busca aprimorar as técnicas para Avaliação e Análise de Riscos Relacionadas às redes de cabos submarinos internacionais.

5.1. TÉCNICAS AVALIADAS NO ESTUDO

Para apresentação de um modelo objetivando aprimorar a utilização da ferramenta RSA-Archer da Anatel foram avaliadas as seguintes técnicas: Análise de Árvore de Falha – AAF (Fault Tree Analysis – FTA), a Análise de Modos de Falhas e Efeitos – AMFE (Failure Modes and Effect Analysis – FMEA) e a Análise de Árvore de Eventos – AAE (Event Tree Analysis – ETA).

5.1.1. FAULT TREE ANALYSIS – FTA

É uma representação gráfica, associada ao desenvolvimento de uma falha particular do sistema (efeito= evento de falha), chamada de Evento de Topo e às falhas básicas (causas= eventos primários).

 Finalidade: Estuda os resultados negativos considerados suficientemente sérios para demandar análise posterior.

- Identificação das causas primárias das falhas
- Elaboração de uma relação lógica entre falhas básicas e falha final do sistema
- Análise da confiabilidade do sistema

Procedimento: O ponto de partida da FTA é uma lista de modos de falha indesejáveis para os quais deseja-se dar alguma solução.

- Identificação do evento de falha detectado
- Relação dessa falha com falhas intermediárias e eventos mais básicos por meio de símbolos lógicos

Entendimento do sistema: Por ser modelo gráfico construído de maneira lógica, a FTA permite a análise conjunta de várias causas que levarão à ocorrência do

Evento de Topo, proporcionando ao analista um maior entendimento operacional do sistema.

Característica principal

- Melhor método para análise individual de uma falha específica
- Foco é dado à falha final do sistema (Evento de Topo)

Etapas

(i) Definir o Evento de Topo;

(ii) Entender o sistema;

(iii) Construir a árvore;

(iv) Avaliar a árvore;

(v) Implementar ações corretivas.

5.1.2. FAILURE MODES AND EFFECT ANALYSIS – FMEA

É uma matriz descritiva dos modos de falhas de componentes individuais do sistema, os efeitos sobre outros componentes e no sistema como um todo, hierarquização em termos de ocorrência, gravidade e detecção, bem como recomendações de correções.

Finalidade: Enquanto a FTA estuda os resultados negativos considerados suficientemente sérios para demandar análise posterior, a FMEA tenta acessar a confiabilidade de cada componente, separadamente.

- Identificação das falhas críticas em cada componente, suas causas e efeitos.
- Hierarquização das falhas
- Análise da confiabilidade do sistema

Procedimento: Enquanto o ponto de partida da FTA é uma lista de modos de falha indesejáveis para os quais se deseja dar alguma solução, a FMEA começa com a identificação dos componentes e, para cada um deles, identifica possíveis modos de falha, efeitos e possíveis causas.

Análise das falhas em potencial de todos os elementos do sistema e previsão de consequências

- Relação de ações corretivas (ou preventivas) a serem tomadas

Entendimento do sistema: Enquanto a FTA, por ser modelo gráfico construído de maneira lógica, permite a análise conjunta de várias causas que levarão à ocorrência do Evento de Topo, proporcionando ao analista um maior entendimento operacional do sistema, a FMEA analisa cada causa de um modo de falha e cada correspondente efeito, separadamente.

Características principais:

- Pode ser utilizada na análise de falhas simultâneas ou correlacionada
- Todos os componentes do sistema são passíveis de análise

Etapas

(i) Definir os componentes;

(ii) Para cada componente: (1) Função ou funções; (2) Modos de falha; (3) Efeitos da falha: em outros componentes e no sistema como um todo; (4) Causas da falha; (5) controles atuais; (6) Índice de ocorrência; (7) Índice de gravidade; (8) Índice de detecção; (9) Índice de Risco= produto dos índices de ocorrência, gravidade e detecção; (10) Recomendações.

Outras características básicas da FMEA:

a) A FMEA é uma ferramenta indutiva de análise.: A análise parte do individual específico (causa= evento de falha) para o geral (efeitos= eventos decorrentes da falha). Uma abordagem indutiva tem como foco um individual específico (evento de falha), a partir do qual se busca determinar as correspondentes consequências no todo (efeitos).

b) Na FMEA o evento de falha é considerado causa de efeitos.

c) A FMEA considera o evento de falha como causa e busca possíveis efeitos.

d) A FMEA é caracterizada como uma ferramenta de baixo para cima (bottom-up).

e) A composição dos efeitos na FMEA é encerrada no nível dos efeitos que se vislumbra acontecerem.

f) O nível de encerramento da composição pode não ser o mesmo em todos os efeitos vislumbrados.

g) Todos os componentes do sistema são passíveis de análise.

h) FMEA hierarquiza as falhas em termos índice de risco, resultante da multiplicação dos índices de ocorrência, gravidade e detecção.

5.1.3. EVENT TREE ANALYSIS – ETA

É uma representação gráfica, com lógica binária (sucesso x falha), de possíveis sequências de eventos (“caminhos” ou “trajetórias”) e respectivos resultados (consequências), decorrentes de um disparador (gatilho= evento de falha).

Finalidade: Enquanto a FTA estuda os resultados negativos considerados suficientemente sérios para demandar análise posterior e a FMEA tenta acessar a confiabilidade de cada componente, separadamente, a ETA identifica e avalia consequências (resultados gerais ou parciais no todo) de possíveis sequências de eventos (“trajetórias”) decorrentes de um disparador (gatilho= evento de falha).

5.2. PROCEDIMENTO SUGERIDO

Enquanto o ponto de partida da FTA é uma lista de modos de falha indesejáveis para os quais deseja-se dar alguma solução e a FMEA começa com a identificação dos componentes e, para cada um deles, identifica possíveis modos de falha, efeitos e possíveis causas, a ETA identifica ramificações e respectivos estados de sucesso e falha para cada ramo, cobrindo todos os subsistemas nos quais acontece a propagação da falha.

Entendimento do sistema: Enquanto a FTA, modelo gráfico construído de maneira lógica que permite a análise conjunta de várias causas que levarão à ocorrência do Evento de Topo, proporcionando ao analista um maior entendimento operacional do sistema e a FMEA analisa cada causa de um modo de falha e cada correspondente efeito, separadamente, a ETA, por ser também um modelo gráfico construído de maneira lógica, permite a análise conjunta das diferentes combinações de sequências de sucesso ou falha de eventos que levarão à ocorrência de determinados resultados e suas respectivas consequências, proporcionando ao analista um maior entendimento operacional do sistema.

Característica principal

- Pode ser utilizada na análise de falhas simultâneas ou correlacionada

Etapas:

(i) Definir o Gatilho;

(ii) Conhecer as características do sistema para identificar possíveis sequências de eventos que levem a perdas;

(iii) Avaliar as consequências, em termos de perdas pessoais, danos materiais, prejuízos por cessação ou diminuição de atividades e impactos ambientais, associadas a cada sequência de eventos identificada;

(iv) Estabelecer barreiras, técnicas ou administrativas, à propagação das sequências de eventos identificadas;

(v) Construir a árvore com a lógica binária de sucesso/falha em cada barreira ou de ocorrência/não ocorrência em eventos adicionais;

(vi) Avaliar a árvore, para identificação de pontos que requeiram análise adicional, inclusive quanto à estimativa de probabilidades associadas;

(vii) Implementar as ações propostas.

Outras características básicas da ETA:

a) A ETA é uma ferramenta indutiva de análise. A análise parte do individual específico (gatilho= evento de falha) para o geral (resultados= consequências dos possíveis caminhos). Uma abordagem indutiva tem como foco um individual específico (evento de falha), a partir do qual se busca determinar as correspondentes consequências no todo (efeitos). Uma abordagem indutiva tem como foco um individual específico (evento de falha), a partir do qual busca-se determinar as correspondentes consequências no todo (efeitos).

b) Na ETA o evento de falha é considerado o início de sequências de eventos que resultam em perdas.

c) A ETA considera o evento de falha como causa inicial e busca possíveis consequências.

O emprego das três das principais ferramentas de confiabilidade podem e devem, sempre que possível, ser utilizadas em conjunto para a análise de falhas. Um modo interessante de comparação entre FTA, FMEA e ETA é tomar um mesmo evento de falha como foco de aplicação das três ferramentas.

De acordo com a matriz tempo – espaço mostrado na figura abaixo, elaborado a partir de notas de aulas do curso de engenharia de produção (Silva, João Mello da), na qual o evento de falha corresponde à posição de cruzamento da linha de espaço

“AQUI” com a coluna de tempo “AGORA”, a FTA e a FMEA são ferramentas estruturais, enquanto a ETA é uma ferramenta sequencial.

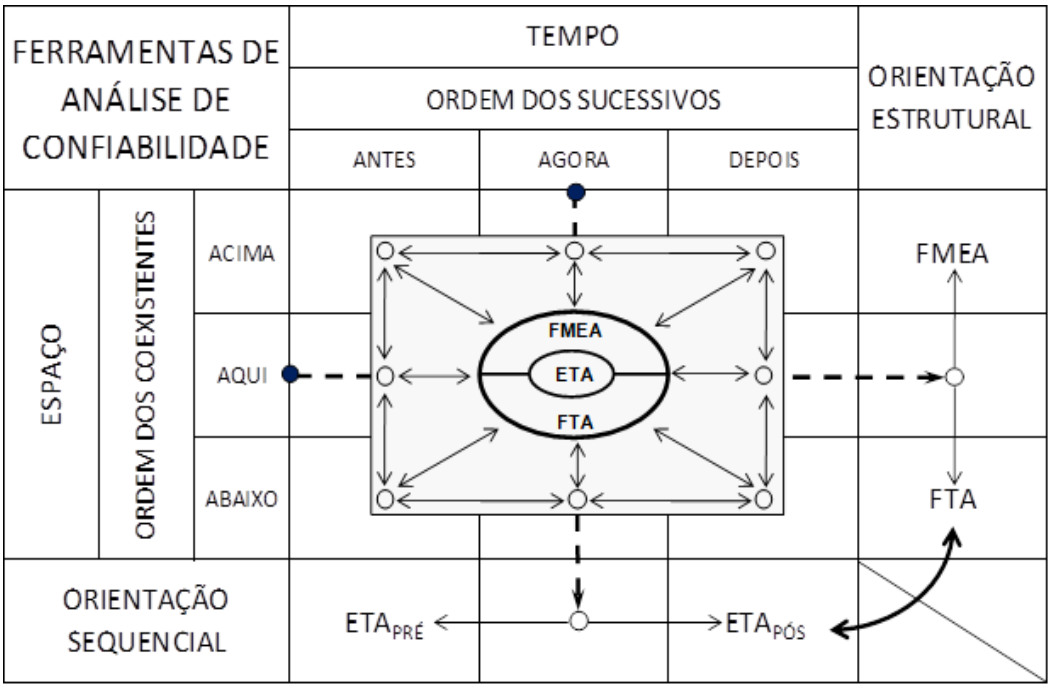


Figura 19 Análise de Confiabilidade.

As setas no retângulo central da matriz, com os deslocamentos elementares (horizontais no tempo, verticais no espaço e transversais, englobando tempo e espaço), indicam, para efeitos de foco em ocorrências específicas, as possíveis movimentações do evento de falha para o posicionamento do evento de falha (AQUI-AGORA) em qualquer posição da matriz.

A partir de um evento crítico (falha) recebida pela ferramenta adquirida pela Anatel, propõe-se avaliar o impacto e afetação (causa-efeito) por meio de uma combinação de fatores (eventos) que representam condições que possam indisponibilizar ou degradar os serviços das Redes de Cabos Submarinos (Causa-Efeito) com intuito de identificar a origem da interrupção ou perda de qualidade (Causa-Raiz), permitindo que as falhas sequenciais no tempo (futuras) possam ser analisadas e sanadas com menor tempo.

Essa ferramenta da qualidade proposta é uma combinação da análise da árvore de falhas, árvore de eventos, causa-efeito e causa raiz. Ela começa a partir de um evento crítico e analisa as consequências que representam condições que podem ocorrer e que levem a falhas ou degradação das redes de cabos submarinos, com intuito de projetar meios que permitam para atenuar as consequências do evento

iniciador. As causas das condições ou falhas são analisadas por meio de árvores de falhas.

A análise de causa e efeito foi originalmente pensada como uma ferramenta de mensuração da afetação da indisponibilidade dos serviços para fornecer um entendimento mais completo das falhas no sistema. Semelhante à análise de árvore de falhas, a análise de causa-raiz é utilizada para representar a lógica da falha que leva a um evento crítico, porém ela se acrescenta à funcionalidade de uma árvore de falha, permitindo que as falhas sequenciais de tempo sejam analisadas.

É utilizado para analisar os vários caminhos que um sistema tomaria após um evento crítico em função do comportamento dos subsistemas específicos (tais como sistemas de resposta de emergência). Se forem quantificados, eles darão uma estimativa da probabilidade de diferentes consequências possíveis após um evento crítico. Como cada sequência em um diagrama de causa e efeito é uma combinação de árvores de subfalhas, a análise de causa e efeito pode ser utilizada como uma ferramenta para construir grandes árvores de falhas.

O Monitoramento das Redes de Telecomunicações está cada vez mais complexo devido ao grande número de diferentes equipamentos e tipos de serviço. A esse aumento de complexidade corresponde um aumento no número de falhas permanentes e/ou transientes e consequentemente, um aumento substancial no número de alarmes devido à interdependência entre os Elementos Gerenciáveis (EG), fazendo com que uma ocorrência primária gere múltiplas ocorrências secundárias. Neste contexto os eventos de falhas podem ser correlacionados, facilitando assim o estabelecimento dos Riscos Inerentes aos transientes de cada serviço.

Há de se observar que, no Caso das Redes de Cabos Submarinos, muitas vezes a falha propagada pelas Redes de telecomunicações, induz, ao receber os alarmes, que “n” pontos dos sistemas foram interrompidos, porém como a falha já chega correlacionada, observa-se um ganho para a descoberta da causa-raiz, diminuindo assim o tempo de indisponibilidade.

A Gerência de Controle de Obrigações da Anatel, ao receber tais alarmes correlacionados, facilmente realiza uma análise rápida e pode executar ações imediatas de comunicação sobre as causas da ocorrência, evitando um possível colapso do sistema.

Desta forma, uma ocorrência grave é geralmente precedida de um aumento de alarmes com características diferentes do comportamento em situações normais. A análise eficiente dos alarmes na identificação das falhas contribui para o aumento da disponibilidade da rede por meio das seguintes ações: Intervenção preditiva, agindo antes da manifestação da falha; Intervenção corretiva, localizando rapidamente a causa do problema.

O procedimento proposto a ser seguido é o seguinte:

- ✓ Identificar o evento crítico (ou iniciador) (equivalente ao evento de topo de uma árvore de falha e o evento inicial de uma árvore de eventos).
- ✓ Desenvolver e validar a árvore de falha quanto às causas do evento iniciador. Os mesmos símbolos são utilizados como na análise da árvore de falha convencional.
- ✓ Decidir a ordem em que as condições devem ser consideradas. Convém que isto seja uma sequência lógica, como a sequência de tempo em que elas ocorrem.
- ✓ Construir os caminhos para o efeito, em função das diferentes condições. Isto é similar a uma árvore de evento, porém a separação em caminhos da árvore de evento é mostrada como uma caixa rotulada com a condição específica aplicável.

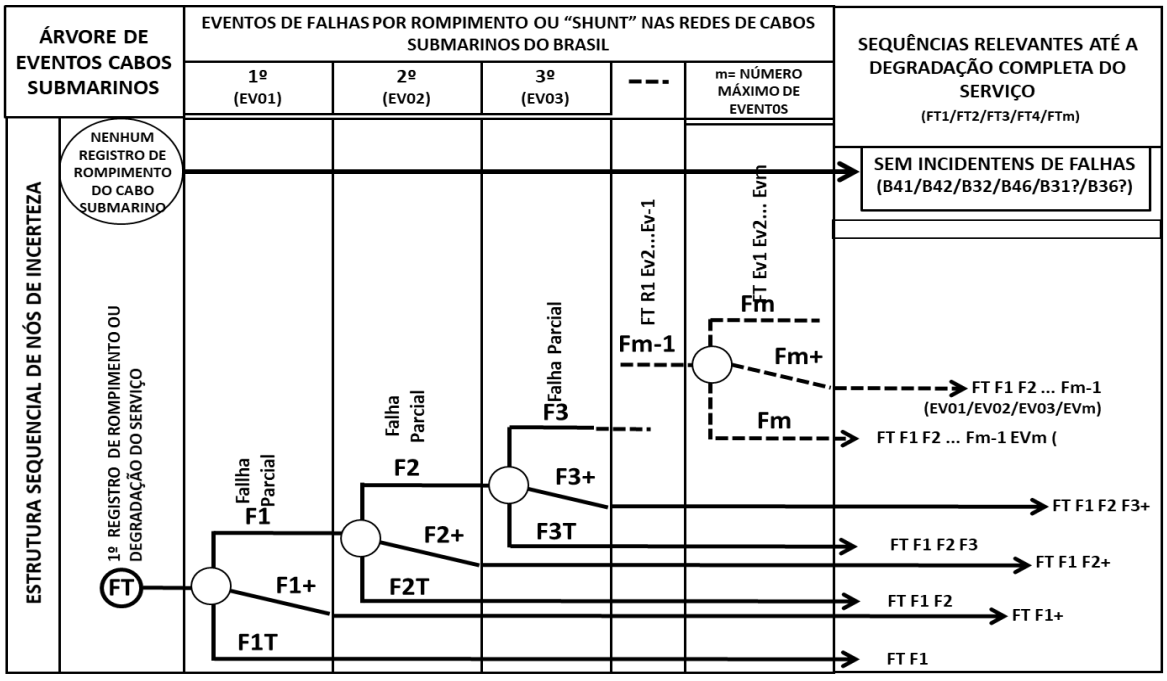


Figura 20 Análise de Falhas.

Conforme a estrutura sequencial de nós de incerteza, elaborado a partir de notas de aulas do curso de engenharia de produção (Silva, João Mello da) e ilustrado na figura 20, e considerando que as falhas para cada caixa de condição são independentes, a probabilidade de cada efeito poderá então ser mensurada. Isto é conseguido em primeiro lugar atribuindo-se probabilidades para cada saída da caixa de condição (utilizando as árvores de falhas pertinentes, como apropriado, parcial ou total).

Observa-se que durante a fase de operação de uma determinada rede de cabo submarino podemos ter falhas totais ou parciais, que degradem a fruição dos serviços, ou ainda a não ocorrência de nenhum evento.

A figura supracitada ilustra as sequências relevantes de eventos de falhas nas redes submarinas e permite observar, por exemplo, que um determinado cabo submarino pode operar durante todo o seu ciclo de vida sem nenhum evento de interrupção.

A saída da análise de causa e consequência é uma representação esquemática de como um sistema pode falhar mostrando tanto as causas como as consequências, além de uma estimativa da probabilidade de ocorrência de cada consequência potencial com base na análise das probabilidades de ocorrência de condições específicas após o evento crítico.

Os pontos fortes e limitações da ferramenta incluem as mesmas vantagens das árvores de evento e árvores de falhas combinadas. Além disso, ela supera algumas das limitações dessas técnicas ao ser capaz de analisar eventos que se desenvolvam ao longo do tempo.

A análise de causa e efeito fornece uma visão abrangente do sistema GRC, que poderá ser configurado atentando-se para o tipo de falha/efeito. A limitação é que é mais complexa do que a análise da árvore de falha e árvore de evento, tanto para construir quanto na maneira em que as dependências são tratadas durante a quantificação.

A preparação da árvore de falhas consiste em um processo probabilístico no qual predomina a análise da relação de causa e efeito existente entre os elementos que compõem um produto ou um processo. Assim, sua elaboração passará sempre pela definição daquilo que se pretende analisar, pelo processo de análise e pela obtenção dos resultados obtidos. Nesse entorno é possível então propor metodologias com maior ou menor grau de detalhamento. De acordo com Helman e

Andery (1995), por exemplo, a sequência de procedimentos para o FTA é definida conforme sintetizado nos Quadros abaixo:

Etapas
1. Definir a equipe responsável no Centro de Operações
2. Selecionar o “evento de topo” das Redes de Cabos Submarinos
3. Coletar dados
4. Definir quais são as interfaces ou fronteiras do sistema
5. Analisar detalhadamente o sistema
6. Montar preliminarmente a árvore de falhas
7. Revisar a árvore de falhas
8. Calcular a probabilidade do evento de topo
9. Analisar as recomendações
10. Refletir sobre o processo

Quadro 3 Etapas FTA.

Descrição das etapas
A equipe deve ser multifuncional
Onde o evento de topo é a falha do sistema que é motivo de estudo
Coletar as informações que serão analisadas
Definir os eventos ou situações básicas cuja análise não se considera necessária aprofundar
Aprofundar a análise detalhada do sistema, buscando compreender suas características e suas inter-relações.
Elaboração de um esboço da árvore de falhas
Revisão e elaboração definitiva da árvore de falhas
O cálculo é feito com o uso de axiomas matemáticos específicos para relações lógicas
Elaborar um plano de ação e analisar se ele está visando ao bloqueio das causas básicas
Verificar se ainda é necessário elaborar outros planos de ação

Quadro 4 Descrição das etapas do FTA.

O uso integrado do FMEA e FTA já foi abordado na literatura por diversos autores podendo se destacar as obras de Helman e Andery (1995), Scapin (1999) e Stamatis (1995). Contudo, o uso integrado destas ferramentas comumente não é discutido em profundidade, principalmente no que se refere às etapas preliminares de sua utilização e ao uso do FTA como recurso de melhoria para o nível de confiabilidade FMEA.

CONCLUSÃO

Após análise dos dados das redes de cabos submarinos, o trabalho apresenta uma proposta de utilização do FTA como ferramenta de apoio ao FMEA e ETA para avaliação dessas redes, especificamente às redes brasileiras. Sugerindo a customização da plataforma RSA Archer para aplicação destes métodos.

Observou-se ainda a necessidade de construção de documentos e políticas consideradas como as linhas mestras para instituir a segurança da informação como prática institucional no que tange as infraestruturas de redes de telecomunicações e que vão ao encontro das necessidades atuais da organização.

Neste sentido, é recomendado a execução de trabalhos que contemplem a elaboração de um plano de gestão de continuidade das redes de cabos submarinos no Brasil, bem como um plano de capacitação em Gestão de Riscos para os colaboradores da agência com intuito de aprimorar o acompanhamento do Regulamento de Gestão de Riscos da Anatel, aprovado por meio da RESOLUÇÃO Nº 656, DE 17 DE AGOSTO DE 2015.

Em pesquisas públicas realizadas de leis, regulamentos ou portarias específicas sobre proteção das redes de cabos submarinos verificou-se a existência do DECRETO N. 9749 - DE 6 DE MAIO DE 1887, aprovado pelo Barão de Cotegipe, que interpreta o cumprimento dos arts. 2º e 4º da Convenção Internacional para a proteção dos cabos submarinos.

Relacionado ao tema citado anteriormente, foi avaliado que em alguns países como Portugal, Nova Zelândia e Austrália, existem leis específicas que tratam da proteção dos cabos submarinos, incluindo restrições de pescas de arrasto nas rotas marítimas que estão instalados os cabos. No Brasil, ficou evidenciado a necessidade de atualização em consonâncias com as legislações de outros países.

Relacionado ao tema de dimensionamento do tráfego de dados das redes brasileiras e projeção de crescimento, faz-se necessária uma nova missão de estudos e avaliações presencialmente naquelas redes com intuito de estudar a situação atual, incluindo a segurança física das instalações.

Por fim, baseados nos estudos realizados durante o trabalho das situações específicas das redes de cabos ópticos submarinos no Brasil, propõe-se que a Agência construa modelos de Gestão de Risco ancorados em três ferramentas de Engenharia de Confiabilidade: (i) Análise de Árvore de Eventos (Event Tree Analysis

– ETA); (ii) Análise de Árvore de Falhas (Fault Tree Analysis – FTA); e (iii) Análise de Modos de Falha e Efeitos (Failure Modes and Effects Analysis – FMEA).

O primeiro passo da modelagem é a elaboração de Diagrama(s) ETA que mostre(m), em uma progressão temporal, a sequência de eventos que evidenciem possíveis intervenções nas redes com suas respectivas probabilidades de sucesso. Em seguida, para cada evento identificado e caracterizado em Diagrama ETA sugere-se o desenvolvimento de Dashboards representando minimamente: (a) Diagrama(s) FTA, para identificação e caracterização lógica das suas causas, em abordagem top-down, com suas respectivas probabilidades de ocorrência; e (b) Diagrama(s) FMEA, para identificar e caracterizar relacionamentos, em abordagem bottom-up, com seus respectivos graus de risco quanto à ocorrência, detecção e severidade.

Percebe-se que a análise quantitativa que se faz através dessas técnicas pode complementar a análise qualitativa do FMEA e que a integração entre essas três ferramentas embasa as análises de falha das Redes, fazendo com que esta tenha menos incertezas com relação à priorização das ações de melhoria que devem ser implementadas.

Recomenda-se ainda que a área de negócios da Anatel, que gerencia os dados recebidos das principais operadoras de cabos submarinos no Brasil, adote as técnicas supracitadas com intuito de aprimorar a análise das redes objeto do trabalho.

Infelizmente, em decorrência da Pandemia ocasionada pelo Covid-19 a proposta não pode ser customizada na ferramenta RSA-Archer, pois o centro de monitoramento das redes de telecomunicações, criado em 2014 pela Agência, encontra-se provisoriamente impossibilitado de receber novas adequações e customizações. Ademais o acesso aos dados das empresas para aplicação da metodologia proposta depende de um pedido formal da área competente em decorrência da segurança e criticidade do compartilhamento desses dados.

Atualmente, o centro monitora em tempo real as interrupções e desempenho dos serviços de voz, banda larga e banda larga móvel das principais operadoras de redes de telecomunicações no Brasil.

Enquanto o Centro de Monitoramento de Redes não recepciona novas implementações, será proposto ao curador de dados das redes de cabos ópticos submarinos no âmbito da Agência a inclusão de um monitoramento das redes de

cabos ópticos submarinos por meio do Painel de Dados da Anatel desenvolvido no Qlik Sense, à exemplo dos Dashboards “meu município” https://informacoes.anatel.gov.br/paineis/meu-municipio e “infraestrutura” https://informacoes.anatel.gov.br/paineis/infraestrutura

A implementação deverá envolver, além dos dados de redes já coletados das principais operadoras no Brasil, integração com dados do site https://www.submarinecablemap.com/ da *TeleGeography* e atualização da topologia das redes com a entrada dos novos *Players.*

Em estudos futuros, sugere-se ainda verificar se o FTA pode também contribuir para a obtenção de índices de ocorrências de falha nas redes de cabos submarinos. Neste caso, indica-se a realização de um estudo específico e atualizado das redes para examinar sua exequibilidade e vantagens de aplicação.

REFERÊNCIAS

ANATEL- Agência Nacional de Telecomunicações. Resolução nº 656, de 17 de agosto de 2015 - Regulamentos sobre Gestão de Risco das Redes de Telecomunicações e Uso de Serviços de Telecomunicações em Desastres, Situações de Emergência e Estado de Calamidade Pública. Disponível em: https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/32407430/do1-2015-08-19-resolucao-n-656-de-17-de-agosto-de-2015-32407336. Acesso em: 25/08/2021.

AS/NZS - Autralian Standard and New Zealand Standards. AS/NZS 4360:2004-RISK MANAGEMENT. Australia / New Zealand, 2004.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS- ABNT**.** Norma Brasileira ABNT NBR ISO/IEC 27002:2013 – Técnicas de Segurança - Código de prática para a gestão da segurança da informação.2009.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS- ABNT. Norma Brasileira ABNT NBR ISO/IEC 31000:2009 – Gestão de riscos – Princípios e diretrizes.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS- ABNT. Norma Brasileira ABNT NBR ISO/IEC 38500:2009 – Governança Corporativa de Tecnologia da Informação.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS- ABNT. Norma Brasileira ABNT ISO/IEC Guia 73:2009 - Gestão de riscos – Vocabulário

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS- ABNT. Norma Brasileira ABNT NBR ISO/IEC 31010:2012 – Gestão de riscos – Técnicas para o Processo de Avaliação de Riscos.

BRASIL. Instrução Normativa SLTI/MP N° 4 de 12 de novembro de 2010. Secretária de Logística e Tecnologia da Informação. Brasília- DF.

BRASIL. Senado. **Relatório Final da CPI da Espionagem**. 2014. Disponível em https://www12.senado.leg.br/noticias/arquivos/2014/04/04/integra-do-relatorio-de-ferraco . Acesso em: 20/08/2021.

BRASIL. Senado. DECRETO n. 9749. **Diário Oficial da União**. Brasília-DF. Disponível em: https://www2.camara.leg.br/legin/fed/decret/1824-1899/decreto-9749-6-maio-1887-543173-publicacaooriginal-53240-pe.html. Acesso em: 30 jun. 2021.

CANONGIA, C.; MANDARINO JR., R., and GONÇALVES JR., A. (eds). Guia de Referência Para a Segurança Das Infraestruturas Críticas Da Informação - Versão 01. Brasília - DF: DSIC/SE/GSI/PR **- Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República**, 2010.Disponível em: http://dsic.planalto.gov.br/documentos/publicacoes/2_Guia_SICI.pdf. Acesso em 05/06/2021.

FERNANDES, Jorge H. C. Proteção de Infraestruturas Críticas de Informação. Curso de Especialização em Gestão da Segurança da Informação e Comunicações - CEGSIC / **Departamento de Ciência da Computação, Instituto de Ciências Exatas, Universidade de Brasília**, Brasília. 2014.

FREITAS, Marta Afonso; COLOSIMO, Enrico Antônio. Confiabilidade: Análise de Tempo de Falha e Testes de Vida Acelerados, Série Ferramentas da Qualidade – Volume 12, Belo Horizonte: Fundação Christiano Ottoni, Escola de Engenharia da Universidade Federal de Minas Gerais, 1997.

GUALBERTO, E. S. Um modelo de informações para gerência de riscos de segurança da informação: aplicação em uma organização pública. Departamento de Ciência da Computação - Universidade de Brasília, 2008.

HELMAN, H.; ANDERY, P. R. P. Análise de falhas: aplicação dos métodos de FMEA e FTA. Belo Horizonte: Fundação Christiano Ottoni, Escola de Engenharia da UFMG, 1 ed., 1995.

LIMA, P. F. A.; FRANZ, L.A.S.; AMARAL, F.G.; **Proposta de Utilização do FTA como Ferramenta de Apoio ao FMEA em uma Empresa do Ramo Automotivo.** Anais do XIII SIMPEP Bauru, SP, Brasil, 06 a 08 de novembro de 2006

IRM – INSTITUTE OF RISK MANAGEMENT: The Association of Insurance and Risk Managers and National Forum for Risk Management in the Public Sector. A Risk Management Standard. EUA: IRM, 2002.

PALACIOS, Mario Sergio. **Cabos Submarinos no Brasil**. TELECO- Inteligências paratelecomunicações. 2003. Disponível: https://www.teleco.com.br/tutoriais/tutorialcsub/default.asp. Acesso em: 4 ago. 2021.

VIANA, Natália. WIKILEAKS divulga lista de locais ‘vitais’ para segurança nacional dos EUA. **Wikileaks**, , 05 dez. 2010. Disponível em: http://wikileaks.org/A-lista-secreta-de-compras-do.html. Acesso em: 21/08/2021.