UNIVERSIDADE FEDERAL DO CEARÁ

CENTRO DE TECNOLOGIA

DEPARTAMENTO DE ENGENHARIA DE TELEINFORMÁTICA

PROGRAMA DE PÓS GRADUAÇÃO EM ENGENHARIA DE TELEINFORMÁTICA

AMINADABE BARBOSA DE SOUSA

ASP - MODELO ORIENTADO AO NEGÓCIO PARA IDENTIFICAÇÃO DE PONTOS CRÍTICOS EM REDES ÓPTICAS

FORTALEZA

2018

AMINADABE BARBOSA DE SOUSA

ASP - MODELO ORIENTADO AO NEGÓCIO PARA IDENTIFICAÇÃO DE PONTOS CRÍTICOS EM REDES ÓPTICAS

Tese apresentada ao Programa de Pós-Graduação em Engenharia de Teleinformática da Universidade Federal do Ceará, como requisito parcial à obtenção do título de Doutor em Engenharia de Teleinformática. Área de concentração: Sinais e Sistemas. Redes de Computadores. *Business-driven IT Management-BDIM.*

Orientador: Prof. Dr. José Neuman de Souza
Coorientador: Prof. Dr. Alberto Sampaio Lima

FORTALEZA

2018

Dados internacionais de catalogação na publicação
Universidade Federal do Ceará
Biblioteca Universitária
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

S696a Sousa, Aminadabe Barbosa.

ASP - Modelo orientado ao negócio para identificação de pontos críticos em redes ópticas Aminadabe Barbosa Sousa. – 2018.

200 f. : il. color.

Tese (doutorado) – Universidade Federal do Ceará, Centro de Tecnologia, Programa de Pós-Graduação em Engenharia de Teleinformática, Fortaleza, 2018.

Orientação: Prof. Dr. José Neuman de Souza.

Coorientação: Prof. Dr. Alberto Sampaio Lima.

1. Redundância. 2. Redes Ópticas. 3. Gestão de TI Orientada ao Negócio. 4. Gerenciamento de Falhas. 5.Gerenciamento de Riscos. I. Título.

CDD 621.38

AMINADABE BARBOSA DE SOUSA

ASP - MODELO ORIENTADO AO NEGÓCIO PARA IDENTIFICAÇÃO DE PONTOS CRÍTICOS EM REDES ÓPTICAS

Tese apresentada ao Programa de Pós-Graduação em Engenharia de Teleinformática da Universidade Federal do Ceará, como requisito parcial à obtenção do título de Doutor em Engenharia de Teleinformática. Área de concentração: Sinais e Sistemas. Redes de Computadores. *Business-driven IT Management-BDIM.*

Aprovada em:_08_/_06_/_18_

BANCA EXAMINADORA

_____
Prof. Dr. José Neuman de Souza (Orientador)
Universidade Federal do Ceará (UFC)

_____
Prof. Dr. Alberto Sampaio Lima (Coorientador)
Universidade Federal do Ceará (UFC)

_____
Prof. Dr. Giovanni Cordeiro Barroso
Universidade Federal do Ceará (UFC)

_____
Prof. Dr. João Batista Rosa Silva
Universidade Federal do Ceará (UFC)

_____
Prof.Dr. Kelvin Lopes Dias
Universidade Federal de Pernambuco (UFPE)

_____
Prof.Dr. José Antão Beltrão Moura
Universidade Federal de Campina Grande (UFCG)

_____
Prof.Dr. Joaquim Celestino Junior
Universidade Estadual do Ceará (UECE)

AGRADECIMENTOS

Sobretudo agradeço a Deus que sempre me deu forças para vencer todas as dificuldades.

O meu agradecimento ao coorientador, professor Alberto Sampaio Lima, por sua importante participação na construção do conhecimento apresentado nesta pesquisa.

Agradeço ao meu orientador, o professor José Neuman de Souza, pelas diversas oportunidades de estudo e aprendizado.

Aos professores participantes das bancas examinadoras, pelas valiosas colaborações e sugestões.

Aos colegas do grupo de pesquisa Germano Fenner, Maristella Ribas e Janete Amaral pelas reflexões, críticas e sugestões recebidas.

A minha esposa Renata pela paciência e incentivo durante o período.

Aos meus pais por sempre terem me incentivado.

A todos que diretamente ou indiretamente contribuíram para a realização deste trabalho.

“Embora ninguém possa voltar atrás e fazer um novo começo, qualquer um pode começar agora e fazer um novo fim.” (Chico Xavier)

RESUMO

As melhores práticas de gerenciamento de serviços tem sido amplamente adotadas por provedores que mantém e administram infraestruturas de redes de computadores. Um dos pressupostos para a adoção dessas práticas consiste na manutenção de um alinhamento efetivo entre a gestão de tecnologia da informação e a gestão do negócio. Entre os desafios que os gestores de serviços enfrentam ao trabalhar com a gestão de redes ópticas, a identificação de pontos de redundância de alto impacto em relação ao negócio é uma tarefa considerada difícil. Muitas vezes, esses gestores dependem de sua própria experiência para identificar os pontos que podem receber investimentos em redundância nessas redes e serem priorizados em relação ao orçamento planejado. Existe uma demanda crescente por novos modelos e ferramentas que possam dar suporte ao processo de tomada de decisão. Esta tese propôs um novo modelo, capaz de localizar pontos adequados para a aplicação da redundância de ativos através de simulações, que tem como objetivo mitigar os riscos de interrupções do funcionamento de uma rede óptica, com foco no negócio. O modelo foi implementado através de uma ferramenta de *software* denominada *Strategic Asset Locator Program(ASP),* que realiza simulações de cenários de redes ópticas, com análise de falhas baseada na topologia, dependência entre elementos de rede e no impacto da falha para o negócio, estimando o risco desses elementos. A saída do modelo (elementos da rede e respectivos riscos) permite que os administradores de rede e serviços tomem melhores decisões ao analisar os riscos e definir quais os pontos críticos passíveis de redundância. Um estudo de caso foi realizado em uma empresa real, por meio de simulações que envolveram cinco cenários de redes de referência, onde os resultados foram avaliados por gestores e considerados promissores, contribuindo assim para a área de pesquisa denominada *Business-driven IT Management (BDIM)*.

Palavras-chave: Redundância. Redes Ópticas. Gerenciamento de Serviços. Gestão de TI. Orientada ao Negócio. Gerenciamento de Falhas. Gerenciamento de Riscos.

ABSTRACT

Best service management practices have been widely adopted by providers who maintain and manage computer network infrastructures. One of the prerequisites for adopting these practices is to maintain an effective alignment between information technology management and business management. Among the challenges service managers face while working with optical networks, identifying network high-impact redundancy points in relation to business is a difficult task. Often these managers rely on their own experience to identify points that can receive investments in redundancy in those networks and need to be prioritized in relation to planned budget. There is a growing demand for new models and tools that can support decision-making process. This thesis proposed a new model, capable of finding suitable points for the application of asset redundancy through simulations, which aims to mitigate optical network operation interruption risks, with a business focus. The model was implemented through a software tool named *Strategic Asset Locator Program (ASP)*, which performs optical network scenarios simulations, with fault analysis based on topology, dependence between network elements and failure impact on business, estimating the risk related to these elements. The model output (network elements and their risks) allows service and network managers to make better decisions when analyzing risks and defining which critical points can be redundant. A case study was carried out in a real company, through simulations involving five reference network scenarios, where results were evaluated by managers and considered promising, thus contributing to Business-driven IT Management (BDIM) research area.

Keywords: Redundancy. Optical Networks. Service Management. Business-driven IT. Management. Fault Management. Risk Management.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS

AHP	*Analytical Hierarquical Process*
BSC	*Balanced Score Card*
BDIM	*Business Driven IT Management*
CCTA	*Central Computer and Telecommunications Agency*
CMMI	*Capability Maturity Model Integration*
COBIT	*Framework for Governing and Managing Enterprise IT*
CRM	*Customer Relation Management*
DS	Dinâmica de Sistemas
ERP	*Enterprise Resource Planning*
ISACA	*Information System Audit and Control*
ISO	*International Organization for Standardization*
ITGI	*IT Governance Institute*
ITIL	*Information Technology Infrastructure Library*
ITSM	Gerenciamento de Serviços de TI
MOF	*Microsoft Operations Framework*
OGC	*Office of Government Commerce*
PDCA	*Plan - Do - Check - Act*
PETI	Planejamento Estratégico da TI
QoS	*Quality of Service*
ROI	Retorno de Investimento
SD	*Service Desk*
SLA	Acordo de nível de serviço
TI	Tecnologia de Informação
SDH	Hierarquia digital síncrona (Synchronous Digital Hierarchy)
AFA-FLA	Alarm Filtering Algorithm-Fault Location Algorithm
PDH	Hierarquia digital plesiôcrona (*Plesyochronous Digital Hierarchy*)
WDM	Multiplexação por divisão de comprimento de onda (*Wavelenght Division Multiplexing*)
DWDM	Multiplexação densa por divisão de comprimento de onda (*Dense-Wavelenght Division Multiplexing*)
CGR	Centro de Gerência de Redes
ITU	*International Telecommunication Union*
ISO	*International Standard Organization*
OSI	Interconexão de sistemas abertos (*Open system Interconnection*)
MIB	Base de Informações de Gerenciamento (*Management Information Base*)
SMI	Estrutura de gerenciamento de informações (*Structure of Management Information*)
SNMP	Protocolo simples de gerenciamento de rede (*Simple Network Management Protocol*)

MIS-Users	Sistema de informação de gerência – usuários (*Management Information Services – Users*)
LME	Entidade de gerenciamento de camadas (*Layer Management Entities*)
SMAE	Entidade de aplicação da gerência de sistemas (*System Management Application Entity*)
RIP	Protocolo de roteamento de informações (*Routing Information Protocol*)
TMN	*Telecommunication Management Network*
LAN	Rede de área local (*Local Area Network*)
WAN	Rede de área extendida (*Wide Area Network*)
SDM	Multiplexação por divisão espacial (*Space Division Multiplexing*)
SGMP	*Simple Gateway Monitoring Protocol*
DNS	Sistema de Nomeação de Domínio (*Domain Naming System*)
DXC	Conexão-cruzada digital (*Digital Cross-Connect*)
STM-N	Módulo de transporte síncrono – N camadas (*Synchronous Transport Module – Level N*)
C	*Contêiner (Container)*
VC	Contêiner Virtual (Virtual Container)
TU	Unidade tributária (Tributary Unity)
TUG	Grupo de unidade tributária (Tributary Unity Group)
AU	Unidade administrativa (Administrative Unity)
AUG	Grupo de unidade administrativa (Administrative Unity Group)
NNI	Interface de nó de rede (Network Node Interface)
SDN	Software Defined Networking
EON	Elastic Optical Networl

LISTA DE SÍMBOLOS

$	Dólar
%	Porcentagem
£	Libra
¥	Iene
€	Euro
§	Seção
©	Copyright
®	Marca Registrada

SUMÁRIO

1. INTRODUÇÃO

A necessidade de manter serviços estáveis em grandes redes gerou uma demanda por novas formas de prevenção de falhas aliadas às demandas das empresas provedoras de serviços. Os sistemas de proteção contra falhas enviam alarmes, provenientes de componentes de rede, que são direcionados para um local de gerenciamento. Neste local, os alarmes são analisados pelos operadores, que tomam decisões para resolver os problemas identificados. Um passo muito importante nessa tarefa consiste na localização da falha. Devido ao alto tráfego de dados que geralmente ocorre em redes ópticas, muitas vezes o número de alarmes enviados por uma falha é muito grande, tornando o trabalho humano bastante complicado e lento (Meira, 1997). Para facilitar a execução desta tarefa, foram propostas soluções denominadas algoritmos de localização de falhas (MAS. *et al.*, 2000a, 2000b; BOULOUTAS *et al*., 1994; LI ; RAMASWAMI, 1997; YEMINI *et al*., 1996; LEE ; CHO, 1998; MÖLLER *et al*., 1995; GARNDNER ; HARLE, 1997; LEHR *et al*., 1998).

Entre os fatores que necessitam ser considerados no gerenciamento de serviços de rede, o estudo do risco comercial envolvido foi destacado como uma das maneiras de encontrar um vínculo mais efetivo entre os níveis de gerenciamento estratégico, tático e operacional. A gestão de riscos deve auxiliar o processo de tomada de decisão (SERGIO *et al*., 2017), a fim de contribuir para um desempenho sustentável do negócio e permitir um maior controle sobre potenciais perdas. O processo envolve os estágios de identificação, avaliação e mitigação de fatores internos e externos capazes de comprometer metas e estratégias corporativas. Cada risco deve ser gerenciado através do uso de metodologias, modelos de medição e controles específicos, gerando ações de mitigação que minimizem seus impactos no negócio.

A decisão sobre quais pontos de rede necessitam de intervenções - incluindo a criação de medidas de redundância - sempre foi um tema de discussão entre os administradores de rede (STEIN, 1999). A necessidade de considerar os aspectos de negócio nessa atividade aumentou consideravelmente o desafio para os gestores de serviços. A pesquisa apresentada nesta tese propõe um modelo para identificar e sinalizar pontos críticos que podem ser redundantes em uma rede óptica, com base no risco para o negócio. A base conceitual para desenvolvimento do modelo proposto incluiu as recomendações dos guias de melhores práticas ITIL (OGC, 2007), COBIT (ISACA, 2005), PMBOK (PMI, 2008), ISO/IEC 27002. O modelo proposto foi implementado através de um *algoritmo* chamado *Strategic Asset Locator Program (ASP)* que analisa possíveis falhas com base na dependência entre os elementos da rede e o

risco para o negócio. Com as informações geradas pelo algoritmo do modelo *ASP*, os administradores de serviços poderão tomar decisões mais assertivas quanto à indicação de pontos críticos, candidatos para a implantação de redundâncias na infraestrutura de rede.

Este documento tem seu conteúdo assim organizado: no Capítulo 2 o contexto geral no qual se insere a contribuição oferecida pelo trabalho de pesquisa é descrito. No Capítulo 3, apresentam-se as teorias que suportam a proposta. No Capítulo 4, descreve-se o modelo e sua forma de utilização. O Capítulo 5apresenta o estudo de caso que buscou por em prática o modelo apresentado e avaliar a sua potencialidade para aprimorar o processo de tomada de decisão. Por fim, o Capítulo 6 apresenta conclusões e discussões sobre trabalhos futuros.

2. CONTEXTO E MOTIVAÇÃO

A rede óptica depende de amplificadores ópticos, laser ou LEDs e multiplexação de divisão de onda (WDM) para transmitir grandes quantidades de dados, geralmente em cabos de fibra óptica, operando a partir de redes de área local (*Local Area Networks - LANs*) ou redes de área ampla (*Wide Area Networks - WANs*). De acordo com Sousa *et. al*. (2005), o nó é o local onde estão localizados os principais dispositivos ópticos como transmissor, receptor, ADFs, entre outros. Um canal é estabelecido quando um nó se comunica com outro nó. Um canal usa um caminho para estabelecer a comunicação de ponta a ponta entre dois nós. Por sua vez, o caminho faz parte de uma trilha, que pode ser, por exemplo, parte de uma topologia de *Ligthtpath* (a topologia de uma rede de comunicação óptica vista pelas camadas da rede de ordem superior).

De acordo com Fen *et al*. (2016), a partir do surgimento de novos serviços, como vídeo de alta definição, áudio em tempo real, vídeo sob demanda e redes privadas virtuais, surgiu uma grande demanda por serviços de redes ópticas e largura de banda. O surgimento de vários problemas de difícil solução nas redes de transmissão tradicionais, tem motivado o desenvolvimento de redes ópticas mais inteligentes, com o objetivo de melhorar o desempenho geral da rede de transmissão, para atender aos requisitos de desenvolvimento de serviços múltiplos e transmissão de alta velocidade, de forma confiável.

Existem 5 modelos de referência bem conhecidos, que podem ser usados na pesquisa de redes ópticas: ARPA2, NFSNET, COST239, USnation e ER_NET. Essas topologias são representativas das topologias de malha populares empregadas no projeto de redes ópticas. As cinco topologias foram consideradas no estudo de caso realizado nesta pesquisa, em cinco cenários simulados (LEE *et al*., 2011; MALIK *et al.*, 2017).

1.1 IDENTIFICAÇÃO DO PROBLEMA

O projeto bem sucedido de uma rede óptica pode ser representado pela capacidade da mesma oferecer os serviços essenciais requeridos por seus usuários e por preservar os seus principais componentes na eventual ocorrência de falhas.

A fim de prevenir eventuais falhas e oferecer alternativas que possam evitar que essas acarretem maiores prejuízos, se faz necessário que os projetos contemplem planos de

redundância e contingência constituídos por uma série de ações e procedimentos que visam soluções e dispositivos de recuperação relacionados a essas falhas. Quando da ocorrência de uma falha em uma rede de médio porte, normalmente uma avalanche de alarmes é enviado para um *dashboard* de gerência (ou *site*). Essa grande quantidade de alarmes dificultará sobremaneira a localização da falha e implicará diretamente no tempo em que os circuitos afetados ficarão indisponíveis.

O impacto financeiro ocasionado pelas falhas às corporações, dependendo do local e do tempo para a recuperação, pode ser devastador. Um dos grandes problemas dos projetos de redes ópticas consiste em uma definição efetiva de pontos que possam receber investimentos em redundância.

Este trabalho pressupõe que as organizações que possuem redes ópticas adotam práticas de gerenciamento de serviços e necessitam tomar decisões com base no seu planejamento estratégico e no cenário de negócios. O modelo proposto nesta tese é específico para suporte ao gerenciamento de falhas em serviços de redes ópticas, considerando a estratégia de organizações provedoras desse tipo de serviço. Foram analisados os processos de gestão de serviços, de forma a se obter um alinhamento entre os objetivos estratégicos dessas organizações e suas necessidades. Foi proposta uma abordagem implementada em uma ferramenta de *software*, que visa gerar informações a partir de simulações de cenários de redes ópticas, relativas às falhas e alarmes emitidos pelos componentes de uma rede de comunicação tradicional, em função do seu respectivo impacto para o negócio. O modelo proposto (ASP) executa a correlação de alarmes, otimizando a identificação de pontos críticos com base no risco e permitindo a modelagem de cenários para contemplar diferentes falhas e análise das melhores soluções para investimento em redundância.

1.2 QUESTÃO DE PESQUISA

Muitas organizações não conseguem realizar decisões mais efetivas em relação à adoção de medidas mitigadoras para os riscos inerentes a suas redes, pelo fato de que seus processos de gerenciamento de serviços, de incidentes, problemas e falhas da rede não estarem alinhados com o planejamento estratégico e as necessidades reais da organização.

Acredita-se que o entendimento sobre as possíveis falhas e um estabelecimento de pontos passíveis de redundância em redes ópticas, pode levar a decisões que favoreçam o alcance dos objetivos estratégicos da empresa. O entendimento do impacto de uma falha de rede no desempenho das atividades pode reduzir o risco do não alcance dos objetivos estratégicos.

Tais pressupostos conduzem às seguintes perguntas de pesquisa: compreender a complexidade que envolve o alinhamento com o negócio e os riscos envolvidos no processo de gerenciamento de falhas em redes ópticas:

- Ajuda a organização na tomada de decisão sobre o quanto investir em pontos de redundância?
- Permite que a empresa priorize os pontos críticos em sua rede óptica?

1.3 OBJETIVOS E CONTRIBUIÇÕES

As organizações tipicamente recolhem informações com a finalidade de avaliar o ambiente empresarial, completando estas informações com pesquisas de marketing, industriais e de mercado, além de análises competitivas. Organizações competitivas acumulam "inteligência" à medida que ganham sustentação na sua vantagem competitiva, podendo considerar tal inteligência como o aspecto central para competir em alguns mercados. Geralmente, os coletores de *BI* (*Business Intelligence* – Inteligência Empresarial) obtêm as fontes primárias de informação dentro das suas empresas. Cada fonte ajuda quem tem que decidir a entender como o poderá fazer da forma mais correta possível. Isto significa que é um método que visa ajudar as empresas a tomar as decisões inteligentes, mediante dados e informações recolhidas pelos diversos sistemas de informação. Sendo assim, BI é uma tecnologia que permite às empresas transformar dados guardados nos seus sistemas em informação qualitativa e importante para a tomada de decisão. Há uma forte tendência de que os produtos que compõem o sistema de BI de uma empresa passem, isoladamente, a prover funções extras que auxiliem na tomada de decisões.

De acordo com Lima (2011), a pesquisa na área de governança de TI tem avançado na busca de soluções efetivas para o problema que envolve o tratamento dos serviços de TI sob o ponto de vista do negócio, entretanto ainda existem lacunas inerentes a esses problemas que não foram resolvidas.

O modelo proposto neste trabalho visa fornecer a alternativa ante as atuais dificuldades nas atividades relacionadas ao gerenciamento de falhas em redes ópticas na visão do negócio. Foca particularmente nos aspectos inerentes à identificação de pontos críticos, passíveis de redundância. Esse modelo é baseado nos princípios de BDIM *(Business Driven IT Management)*. O escopo dos testes no trabalho avaliou simulações de 5 cenários de redes de referência, por meio de estudo de caso em uma empresa real. Como resultados produzidos, foram apresentados: fundamentação teórica que suporta o modelo, duas definições para estimar o impacto de um elemento de rede no contexto do problema, a definição para estimativa do risco de cada elemento de rede, bem como um processo para utilização do modelo (que envolve os gestores).

O objetivo geral e os objetivos específicos que norteiam a realização desta pesquisa são declarados a seguir.

1.3.1 Objetivo Geral

O objetivo geral desta pesquisa foipropor um modelo para suportar o processo de tomada de decisão relativo à identificação e priorização de pontos críticos em redes ópticas, passíveis de redundância, através de simulações de cenários e risco envolvido para o negócio.

1.3.2 Objetivos específicos

A partir do objetivo geral, os seguintes objetivos específicos foram estabelecidos, considerando-se como escopo as empresas que administram redes ópticas:

- Desenvolver um modelo de simulação que possibilite suporte ao processo de gerenciamento de falhas da organização por meio de simulações;
- Validar a utilidade do modelo como ferramenta de apoio aos gestores na tomada de decisões estratégicas sobre investimento em redundância de recursos de rede, através de estudo de caso.

1.3.3 Contribuições do trabalho

A principal contribuição desta tese é o modelo para identificação de pontos críticos em redes ópticas em uma abordagem orientada ao negócio.

Dentre as contribuições apresentadas na pesquisa que resultou neste documento, pode-se destacar a descrição do processo e métodos que levaram à proposta do modelo e *ferramenta de software ASP*, que possibilitam a simulação de cenários de redes ópticas, com objetivo específico de identificar os pontos mais críticos passíveis de redundância, fornecendo suporte ao processo de tomada de decisão.

O modelo possibilita a execução de simulações periódicas, com *feedback* estratégico continuado, fundamentado na mitigação dos riscos envolvidos no processo de gerenciamento de falhas. A camada inferior do modelo trata de detecção e isolamento de falhas, uma subárea da engenharia de controle, com soluções documentadas a partir da literatura que aborda o domínio de alarmes, com a identificação dos elementos de rede e sua quantidade de alarmes em cada simulação realizada. Foi proposto um *design* não intrusivo para as intervenções no processo de gerenciamento de falhas, o que facilita o alinhamento entre TI e o negócio nessa atividade.

2 FUNDAMENTAÇÃO TEÓRICA

Este capítulo apresenta conceitos e teorias que deram suporte ao modelo proposto na presente tese, bem como os trabalhos relacionados. Um trabalho que envolve suporte ao processo de tomada de decisão e ações estratégicas por parte dos gestores, deve considerar o envolvimento de toda a organização para a consecução dos objetivos de negócio. O presente trabalho considerou três níveis hierárquicos para a realização dos seus estudos:

1. Nível Estratégico – Foi considerada a participação de gestores de unidades de negócio da empresa, seus objetivos e acompanhamento estratégico. Foi considerado também a existência de planos estratégicos e seu monitoramento.
2. Nível Tático – É considerado o envolvimento de pessoas com cargos de gestão e que tem o papel fundamental de servir como elo entre a alta administração e as pessoas que executam ações, ou seja, tarefas e serviços. Esses gestores de nível intermediário têm o desafio de transformar a estratégia, definida pela alta direção, em ações práticas e exequíveis que deverão ser executadas pelos colaboradores da organização.
3. Nível Operacional – Formado pelas pessoas que executam as tarefas operacionais. Dotadas de conhecimento técnico, elas são fundamentais para que a empresa consiga ofertar os serviços de TI para seus usuários, os clientes.

2.1 GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO

Nos últimos anos, o termo governança tem ganhado a atenção das organizações devido a necessidade de adotar uma abordagem para responder as exigências e desafios dos negócios globais. Diversas áreas estão tendo algum tipo de intervenção para gerar melhorias. São intervenções que vão desde a criação e estabelecimento de padrões, modelos de processos, documentações até alternativas para criação de indicadores de desempenho.

De acordo com Weill e Ross (2006), a governança de TI consiste na especificação dos direitos decisórios e do *framework* de responsabilidades para estimular comportamentos desejáveis na utilização da TI. Mediante essa prática, pode-se identificar quem toma as decisões sobre TI e contribui para essas decisões, procurando-se aliar os princípios de governança corporativa à utilização da TI para atingir metas corporativas. Lima (2011) afirma que os principais mecanismos de governança de TI consistem nos comitês, processos orçamentários, aprovações, entre outros. A Figura 1 mostra o contexto da governança de TI no modelo de governança corporativa apresentado por Weill e Ross (2006), ao encarar os ativos de informação e tecnologia da informação como um dos principais ativos de uma empresa.

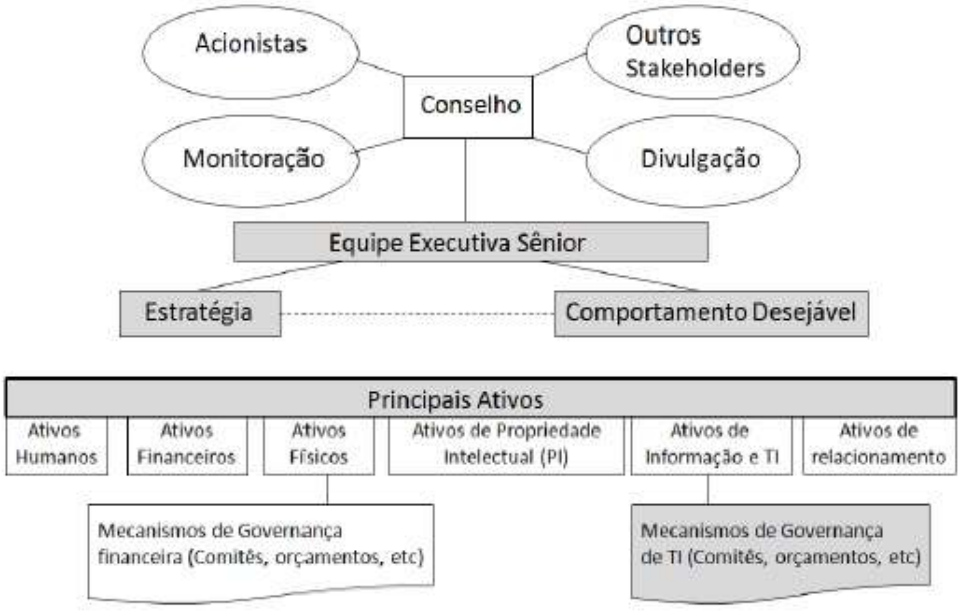


Figura 1. Governança Corporativa e dos principais ativos de uma empresa. Weill e Ross (2006)

Existem algumas consequências indesejáveis relativas ao crescimento do investimento em TI sob o ponto de vista do negócio. A primeira consiste no estado de risco permanente, em razão do crescimento da dependência entre a operação do negócio e o bom funcionamento dos recursos de TI, nos quais suas atividades estão apoiadas. A segunda e mais grave das consequências consiste na incerteza do retorno de todo esse investimento feito em TI, em virtude do relativo grau de intangibilidade associado aos serviços de TI e os benefícios efetivamente produzidos para o negócio (OLIVEIRA, 2010).

Para o IT *Governance Institute* (ITGI), governança de TI é um conjunto de estruturas e processos que visa garantir que a TI suporte e maximize adequadamente os objetivos e estratégias de negócio da organização, adicionando valores aos serviços entregues, balanceando os riscos e obtendo o retorno sobre os investimentos em TI.

Para se entender, projetar, comunicar e sustentar uma governança eficaz é sugerido por Weill e Ross (2006) a utilização de um *framework* de governança de TI mostrado na Figura 2, que ilustra a harmonização entre estratégia e organização, os arranjos de governança de T.I e sua integração com as metas de desempenho do negócio.

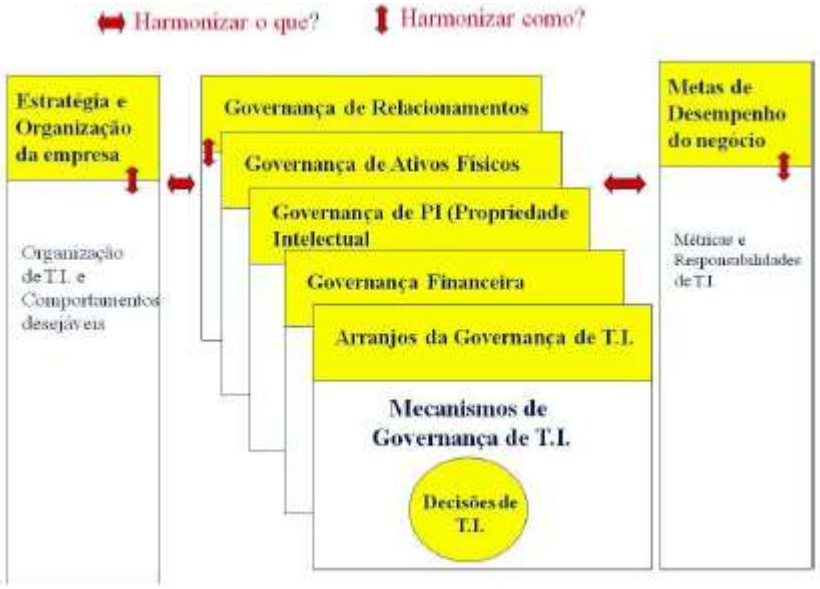


Figura 2. ***Framework*** **de Governança de TI. Weill e Ross (2006).**

A governança de TI busca o alinhamento da TI com a missão da organização, objetivos estratégicos e resultados esperados, além de minimizar os riscos de TI. Os cenários altamente competitivos forçam os patrocinadores do negócio, principalmente os executivos da área

financeira (*CFOs*) e os altos executivos (*CEOs*), a pressionarem as áreas de TI de várias formas, entre elas a cobrança de índices de controle de custos, lucros e alinhamento com o negócio. Essas crescentes pressões chegam aos níveis operacionais dos departamentos de TI e têm forçado os gestores a mudar alguns de seus processos (SAUVÉ *et al*., 2006).

De acordo com Weill e Ross (2006), as empresas de maior desempenho agem por meio da definição de estratégias de negócios claras, avaliando o papel da TI em concretizá-las, pela mensuração e gerenciamento dos investimentos e ganhos obtidos com a TI. Mediante a atribuição de responsabilidades pelas mudanças organizacionais necessárias para se tirar proveito dos novos recursos de TI, e pelo aprendizado com cada implementação, essas empresas tornam-se mais hábeis em compartilhar e reutilizar seus ativos de TI. Na governança de tecnologia da informação, existem cinco decisões inter-relacionadas: os princípios de TI, a arquitetura de TI, a infraestrutura de TI, as necessidades de aplicações do negócio e os investimentos e priorização da TI. Uma das decisões mais importantes na governança de TI se refere à infraestrutura de tecnologia da informação. Entre os serviços compartilhados de TI, incluem-se os serviços de acesso às redes e utilização dos computadores, além dos acessos às aplicações compartilhadas e específicas de negócios da empresa. O alinhamento da TI com o negócio é um aspecto abordado em todas as decisões na governança de TI.

A implantação da governança de TI nas empresas tem sido demandada tanto pelo ponto de vista legal, onde empresas com capital aberto e instituições financeiras estão sendo direcionadas para essa necessidade, quanto pelo ponto de vista do mercado, onde se vive um momento no qual todas as empresas já pensam em como fazer uma implantação efetiva de governança. Entretanto essa não é uma atividade fácil. Muitas empresas não tem conseguido sucesso nesse processo, por conta das inúmeras dificuldades inerentes, além das lacunas de pesquisa que ainda precisam ser resolvidas.

Segundo Abreu e Fernandes (2006), a governança corporativa de TI está inserida na governança corporativa da organização e é dirigida por esta, e busca o direcionamento da TI para atender ao negócio e o monitoramento para verificar a conformidade com o direcionamento tomado pela administração da organização. Ela não é de responsabilidade exclusiva dos gestores de TI e, sim, da alta administração (*board*). A governança de TI é responsabilidade dos executivos e da alta direção da empresa, consistindo em aspectos de liderança, estrutura organizacional e processos que garantam que a área de TI da organização suporte e aprimore os objetivos e as estratégias da organização. É responsabilidade da

governança de TI integrar e institucionalizar boas práticas para garantir que os objetivos de negócios sejam suportados. Por meio de uma boa governança de TI, torna-se possível obter vantagens da informação, maximizando os benefícios, aumentando as oportunidades e ganhando poder competitivo. A governança de TI deve envolver os executivos, a alta direção, nas tomadas de decisões relacionadas ao uso da TI no negócio. É fundamental que exista a participação dos gestores de TI no processo corporativo de tomada de decisão.

No gerenciamento de serviços de TI, o interesse consiste no fornecimento de serviços e produtos de TI, bem como no gerenciamento das operações de TI, enquanto na governança de TI, o interesse está voltado para as operações e desempenho do negócio da empresa. A Tabela 1 mostra uma relação entre gerenciamento de serviços e governança de TI.

Tabela 1 - Diferenças entre o gerenciamento e a governança de TI

Gerenciamento de serviços de TI	Governança de TI
• Suporte ao usuário • Desempenho de serviços • Problemas de infraestrutura	• Alinhamento estratégico • Suporte a estratégia da empresa • Infraestrutura a estratégia da empresa

O gerenciamento de serviços de TI foca em fazer as coisas da forma certa e este serviço é promovido e gerenciado pela área de TI. A governança de TI se preocupa em fazer as coisas certas em relação às operações do negócio da empresa e esse serviço é patrocinado pela alta direção da organização. As ações de gerenciamento de serviços de TI e de governança de TI devem estar alinhadas com as necessidades do negócio.

A área de TI conta com o suporte de diversos *frameworks* disponíveis no mercado. Áreas como desenvolvimento de sistemas, serviços, segurança, qualidade de *software*, projetos, desenvolvimento ágil, todas contam com diversas alternativas desenvolvidas por organizações de referência como ITGI, EXIN, IPMA, ISACA, Microsoft, PMI, *Scrum Aliance*, entre outros.

2.1.1 O guia de melhores práticas COBIT

O COBIT foi a primeira iniciativa desenvolvida para a criação de um padrão que possibilita aos profissionais da TI obterem orientações sobre o que fazer para desenvolver e aplicar a governança de TI dentro das organizações. Atualmente se encontra em sua quinta versão, utilizada como referência na presente pesquisa. Desenvolvido pela *Information Systems Auditand Control* (ISACA, 2015), consiste em um guia, estruturado como *framework*, que possui uma série de componentes que podem ser usados como modelo de referência para gestão de TI. O COBIT pode ser utilizado como alternativa visando a otimização dos investimentos de TI como, por exemplo: melhorar o retorno de investimento (*ROI)* com a utilização de indicadores de desempenho para avaliação de performance e dos resultados.

O COBIT também pode ser usado para avaliar o nível de maturidade da empresa. A utilização do COBIT independe do tipo da plataforma de TI, do tipo de negócio e da participação que a TI tem na empresa. O COBIT v.5 ajuda as organizações a criarem valor para TI, mantendo o equilíbrio entre a realização de benefícios e a otimização dos níveis de risco e o uso de recursos. Têm como objetivos:

- Oferecer um *framework* abrangente que auxilia as organizações a otimizar o valor gerado pela TI;
- Permitir que a TI seja governada e gerenciada de forma holística para toda a organização;
- Criar uma linguagem comum entre TI e negócios para a governança e gestão de TI corporativa

A sigla COBIT significa *Framework for Governingand Managing Enterprise* IT, ou seja, um modelo de negócio para a governança e gestão de TI da organização. Por ser um *framework* aceito mundialmente o COBIT acumulou um histórico de evolução e será mostrado a seguir.

- 1996 - COBIT Versão 1.0 – A ISACA lança a primeira edição do COBIT, um conjunto de objetivos de controle para as aplicações de negócio. A primeira versão tem foco na auditoria.
- 1998 - COBIT 2 – Incluiu uma ferramenta de suporte à implantação e à especificação de objetivos de alto nível de detalhe. A segunda versão tem foco no controle.

- 2000 - COBIT 3 – Incluiu normas e guias associados ao gerenciamento da TI. Na terceira versão, a ISACA deixa de atuar e o ITGI passa a ser o principal editor. A terceira versão tem foco no gerenciamento.
- 2005 - COBIT 4 – É acrescentada melhorias dos controles para assegurar a segurança e a disponibilidade dos ativos de TI na organização. Houve uma redução de 318 para 215 objetivos de controle. A quarta versão tem foco na Governança de TI.
- 2007 - COBIT 4.1 – Houve o agrupamento de alguns objetivos de controle para evitar sobreposições de conceitos e torná-los mais consistentes. Alguns conceitos foram melhorados. A versão 4.1 passou de 215 para 210 objetivos de controle.
- 2011 - COBIT 5.0 – Esta atende as atuais necessidades das partes interessadas a melhorar o alinhamento entre a Governança Corporativa e as técnicas de gestão de TI. COBIT 5 irá consolidar e integrar COBIT 4.1, Val IT, *Risk* IT e também um número significativo de Modelo de Negócios para Segurança da Informação (IMC) e ITAF.

Assim como a biblioteca ITIL, o COBIT 5 é complexo e formado por diversos produtos, guias, com ênfase em assuntos específicos como processos, segurança da informação, riscos entre outros. Segundo a ISO/IEC 38.500, a governança corporativa de TI está envolvida na avaliação, direção e monitoração do uso da TI.**Avaliar (*Evaluate*)** - diretores devem avaliar o uso atual e futuro da TI, incluindo as estratégias, propostas e arranjos de fornecimento (interno, e externo); **Dirigir (*Direct*)** - diretores devem atribuir responsabilidades para a preparação e implementação dos planos e políticas que estabelecem o direcionamento dos investimentos nos projetos e operações de TI; **Monitorar (*Monitor*)** - diretores devem monitorar o desempenho da TI por meio de sistemas de mensuração apropriados, garantindo que esse desempenho esteja de acordo com os planos e objetivos de negócio e que a TI esteja em conformidade com as obrigações externas e práticas internas de trabalho.

Os focos de governança considerados na presente pesquisa foram:

- **Alinhamento estratégico** – foco na garantia de alinhamento entre negócio e TI;
- **Entrega de valor** – foco nas contribuições da TI para objetivos do negócio;

- **Gerência de risco** – foco na comunicação e no controle dos riscos advindos da TI;
- **Gerência de recursos** – foco na contribuição para melhor eficiência dos recursos aplicados na TI;
- **Medição de desempenho** – foco no registro, na comunicação e no controle do desempenho nas atividades de TI.

2.1.2 Gestão de ti orientada ao negócio

O termo *Business-driven IT management* - *BDIM* (gestão de TI orientada ao negócio) consiste na aplicação de um conjunto de modelos, práticas, técnicas e ferramentas para mapear a avaliar quantitativamente interdependências entre o desempenho do negócio e as soluções de TI e usar a avaliação quantitativa para melhorar a qualidade de serviço das soluções de TI juntamente com os resultados dos negócios relacionados (SAUVÉ *et al*., 2006). *BDIM* é uma área de pesquisa recente, relacionada ao gerenciamento de TI. Conforme Bartolini (2009), as aplicações de *BDIM* podem ser executadas em cinco etapas:

1. Identificação de objetivos de negócio e métricas de negócio de interesse para o modelo;
2. Seleção de métricas de desempenho no contexto do cenário de interesse de gerenciamento de TI;
3. Modelagem das entidades relevantes no cenário de interesse;
4. Validação do modelo para tomada de decisão relacionada às soluções de TI;
5. Avaliação de ganhos para o negócio no cenário de interesse escolhido.

Quando todas as etapas são automatizadas, o controle *BDIM* pode ser encapsulado em uma infraestrutura computacional automatizada que permita autogerenciamento on-line de uma aplicação (BARTOLINI, 2009). Bartolini (2009) ainda afirma que existem três domínios de aplicação de *BDIM*: computação autônoma, gerenciamento de serviços de TI e governança de TI. Em cada um destes domínios podem ser encontrados exemplos de soluções *BDIM* relacionadas ao tratamento de problemas de automação e suporte à decisão. No domínio de gerenciamento de serviços de TI, ambos os problemas são tratados. A Figura 3 apresenta o espaço ocupado pelos problemas *BDIM* nos três domínios citados.

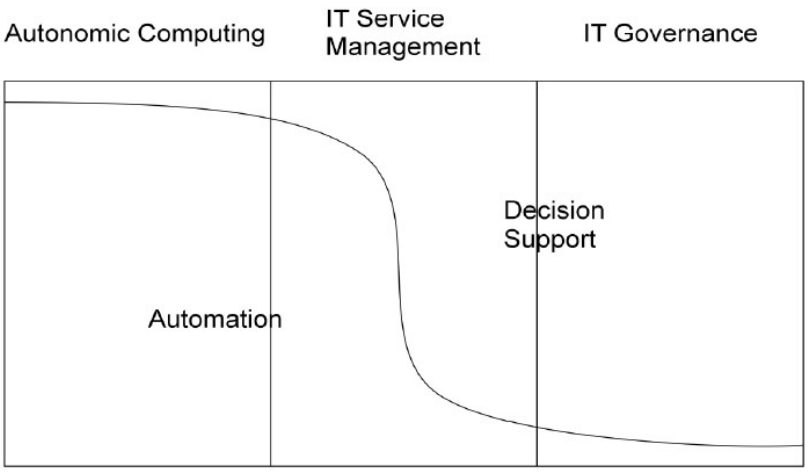


Figura 3. Um espaço de possíveis aplicações BDIM. Bartolini (2009)

Os desafios enfrentados na construção de modelos BDIM são descritos a seguir:

a. desafio da reusabilidade: as diferentes e variadas características dos possíveis cenários de TI e os vários processos de gerenciamento de TI dificultam o desenvolvimento de modelos BDIM genéricos e abrangentes;
b. desafio da precisão do modelo: conseguir valores apropriados e exatos para utilizar como parâmetros do modelo é uma tarefa bem difícil, se eles têm que ser obtidos da mineração de dados históricos ou obtidos de especialistas e usuários;
c. desafio da análise preditiva: fazer previsão de cenários da infraestrutura de TI, depende de componentes da infraestrutura, da carga de trabalho, das pessoas envolvidas, de cronogramas de implantação de serviços, dos processos de negócio afetados, etc;
d. desafio da análise de riscos: a previsão das consequências da utilização de modelos BDIM precisará provavelmente incluir a análise dos riscos por um período de observação bastante longo;
e. desafio da modelagem dos custos: Os custos de modelagem devem ser mantidos no menor nível possível.

De acordo com Lima (2011), os recursos tecnológicos podem pertencer ao nível estratégico, ao tático, ou ao operacional. O nível operacional está relacionado diretamente à infraestrutura da operação, a qual suporta toda a atividade da empresa. A infraestrutura que dá suporte às atividades da empresa, por conta de restrições financeiras, tem uma capacidade limitada. É necessário que haja otimização dessa infraestrutura para o acompanhamento das

constantes evoluções das necessidades do negócio, em especial nos ambientes de corporações virtuais. Para atingir esta meta, deve-se descrever tanto a relação entre a organização e seus processos de negócio quanto as relações entre esses processos de negócio (*BP - Business Process*) e os seus recursos. Portanto, torna-se relevante a elaboração de um modelo global que ligue processos e recursos.

Modelos *BDIM* podem ser utilizados em ferramentas *what-if* para auxiliar a tomada de decisão sobre aquisição, alocação, balanceamento e modernização de ativos de TI. Modelos *Business Process Management (BPM)* podem ser ajustados utilizando-se requisitos *BDIM*, por meio de refinamentos em entidades e camadas do modelo BPM. Outra aplicação de *BDIM* é na modelagem do comportamento das pessoas que trabalham na TI. Questões ligadas a produtividade, esforço do trabalho humano e custos de recursos humanos podem ser estudadas com modelagem *BDIM*.A partir da abordagem BDIM, pode-se realizar pesquisas que envolvem uma grande abrangência de problemas e técnicas na área de computação.

Algumas propostas para o estudo da relação entre a TI e o negócio em *BDIM* foram apresentadas na literatura, tais como teoria das filas (KLEINROCK, 1975), teoria da disponibilidade (KEUS e MARKUS, 1994), teoria da utilidade (READ, 2004), matemática de intervalos (MAREK, 2003), teoria das possibilidades (ZADEH, 1978), dentre outras. Soluções para gerência de incidentes (BARTOLINI e SALLÉ, 2008), gerência de nível de serviço (SAUVÉ e MARQUES, 2005), gerência de portfólio (MOURA, 2008) e de gerência de capacidade (MARQUES *et al*., 2009) são alguns exemplos em que resultados relevantes são obtidos, permitindo que as decisões da governança produzam resultados otimizados do ponto de vista do negócio.

2.1.3 Gerenciamento de serviços

Esta tese aborda aspectos de serviço e estratégia que envolvem redes ópticas. Foi utilizado como referência conceitual, o guia de melhores práticas denominado *Biblioteca de Infraestrutura de Tecnologia da Informação* (*Information Technology Infrastructure Library-ITIL*) (OGC, 2007).

O ITIL é o *framework* para gerenciamento de serviços de TI (*IT Service Management - ITSM*) mais adotado a nível mundial. A utilização das melhores práticas contidas na versão atual do modelo (v. 3), ajuda as organizações a atingirem seus objetivos de negócio utilizando apropriadamente os serviços TI. O modelo ITIL é independente de tecnologia e sua ideia central é trazer uma coleção das melhores práticas, processos e recomendações para o gerenciamento de serviços de TI. A biblioteca ITIL em sua versão atual é composta por cinco livros:

- *Service Strategy* (Estratégia do serviço)
- *Service Design* (Projeto de serviço ou Desenho de serviço)
- *Service Transition* (Transição do serviço)
- *Service Operation* (Operação do serviço)
- *Continual Service Improvement* (Melhoria contínua do serviço)

O ciclo de vida de um serviço é organizado em etapas e estágios, como a estratégia do serviço, onde ocorre a definição dos requisitos e necessidades do negócio, a etapa de projeto de serviço. Na etapa de desenho do serviço (*service design*), é realizada a definição da solução a ser adotada. Já na etapa de transição de serviço *(service transition)*, realiza-se o gerenciamento de mudanças, a etapa de operação do serviço *(servisse operation)*, que busca assegurar que os serviços estão sendo atendidos com base nos acordos de nível de serviço (*Service Level Agreements - SLAs*), estabelecidos. Como indicado por sua denominação, a etapa de melhoria contínua do serviço (*continual servisse improvement)* tem seu foco na qualidade dos serviços entregues, buscando manter uma melhoria constante nesses serviços, através de um ciclo denominado PDCA (*Plan - Do - Check - Act*), o qual envolve atividades de planejamento, execução, monitoramento, retroalimentação e controle. Conforme assevera Lima (2011), o ciclo PDCA é muito importante em dois pontos da melhoria contínua de serviços: implementação de melhorias contínuas dos serviços e aplicação a serviços e seus processos de gerenciamento. Na implementação, todos os quatro estágios do ciclo PDCA são utilizados. Com o aumento da melhoria, a melhoria contínua de serviços gravita em torno dos estágios de checagem (*check*) e ação (*act*) para monitorar, medir, revisar e implementar iniciativas. O ciclo é sustentado por uma abordagem de gerenciamento orientada a processos, onde existem processos definidos, medição de atividades para atendimento do valor esperado e saídas auditadas para validar e melhorar os processos.

Entre os principais benefícios obtidos pelas organizações que utilizam as melhores práticas recomendadas pelo guia ITIL, pode-se citar:

- Alinhamento dos serviços com as necessidades atuais e futuras do negócio. Os processos da ITIL apregoam a necessidade de entendimento dos requisitos de negócio, no sentido de planejamento e entrega de serviços que agreguem valor;
- Melhoria da qualidade dos serviços, através de um programa de melhoria contínua, buscando manter uma consistência na entrega dos serviços e o atendimento das necessidades do negócio;
- Redução dos custos envolvidos na entrega dos serviços; e
- Busca de processos mais eficientes e eficazes, ágeis e com bom desempenho.

Gerentes de TI responsáveis por aspectos de processos em ITSM muitas vezes se deparam com escolhas difíceis. A complexidade dos sistemas de TI e das redes é tanta que algumas vezes uma decisão é tomada mesmo se tendo um conhecimento muito superficial sobre o entendimento dos vários componentes de TI e suas interações, bem como das consequências a que algumas ações tomadas podem levar. Na maioria das vezes, os gestores de TI não sabem como comparar as consequências de ações diferentes, e isso torna uma escolha difícil (SAHAI *et al*., 2008).

Dentre as dificuldades cotidianas enfrentadas pelos gestores de serviços, pode-se citar:

- A deficiência e a dificuldade de se estabelecer um alinhamento entre a estratégia do negócio com as ações da TI.
- A ausência de planejamento estratégico tanto da organização quanto da área de TI.
- A falta de iniciativa que possibilite estabelecer um alinhamento estratégico entre organização e TI.
- Dificuldade em se ajustar os recursos da TI em conformidade com a dinâmica das demandas da organização.
- Alto grau de investimento em recursos de TI sem a devida análise das demandas, dos riscos e benefícios envolvidos, ou sem o alinhamento desta iniciativa com os objetivos da organização.
- Ausência de processos de gestão em TI.
- Ausência de governança de TI.

Segurança da informação (SI) é um tema que ganhou corpo nos últimos anos, obtendo espaço nas mídias e tornando-se *commodity*, em empresas dos mais variados portes e segmentos. Em contrapartida é importante frisar que a popularização do termo SI foi motivada pela elevação no número de incidentes de segurança, ocorridos em âmbito mundial. Os transtornos gerados por esses incidentes são variados gerando, desde danos a imagem do negócio, vazamento de informações críticas, podendo acarretar em perdas financeiras substanciais.

O aumento do número de ocorrências influencia na percepção de valor sobre investimentos em SI, e fazem com que empresas busquem a estruturação de processos para garantir que seus negócios estejam protegidos contra os mais variados tipos de ameaças virtuais.

Em meio a este cenário, surgiu a norma internacional *NBR ISO/IEC 27002* (antigo padrão ISO 17799:2005), que foca nas boas práticas para a gestão da segurança da informação. Nos dias de hoje, ela é fundamental para a consolidação de um *Sistema de Gestão de Segurança da Informação (SGSI)*, garantindo a continuidade e manutenção dos processos de segurança, alinhados aos objetivos estratégicos da organização (ABNT, 2005).

Através do fornecimento de um guia completo de implementação, a norma descreve como os controles podem ser estabelecidos. Esses controles, por sua vez, devem ser escolhidos com base em uma avaliação de riscos dos ativos mais importantes da empresa. A ISO 27002 pode ser utilizada para apoiar a implantação do SGSI em qualquer tipo de organização, pública ou privada, de pequeno ou grande porte, com ou sem fins lucrativos; e não apenas em empresas de tecnologia.

O principal objetivo da ISO 27002 é estabelecer diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização. Isso também inclui a seleção, a implementação e o gerenciamento de controles, levando em conta os ambientes de risco encontrados na empresa.

Entre as vantagens proporcionadas pela adoção da ISO 27002, pode-se citar:

- Melhor conscientização sobre a segurança da informação;
- Maior controle de ativos e informações sensíveis;
- Oferece uma abordagem para implantação de políticas de controles;
- Oportunidade de identificar e corrigir pontos fracos;
- Redução do risco de responsabilidade pela não implementação de um SGSI ou determinação de políticas e procedimentos;

- Torna-se um diferencial competitivo para a conquista de clientes;
- Melhor organização com processos e mecanismos bem desenhados e geridos;
- Promove redução de custos com a prevenção de incidentes de segurança da informação;
- Conformidade com a legislação e outras regulamentações.

2.1.4 Gerenciamento de Incidentes, Problemas e Falhas

De acordo com os conceitos apresentados no ITIL (OGC, 2007), um incidente consiste em uma interrupção não planejada de um serviço de TI ou uma redução da qualidade de um serviço de TI. Uma falha de um item de configuração que ainda não tenha impactado um serviço de TI também é considerada um incidente.

Uma falha é uma condição anormal persistente que requer ação de reparo imediata (ex. Interrupção em um *link* de comunicação). Um erro é uma condição anormal ocasional (por exemplo, erro de *bit* ou falha de sincronização em um *link* de comunicação). O gerenciamento de falhas inclui monitoramento de recursos, verificação do ponto de rede e quando uma falha ou erro pode ocorrer. Os gestores precisam isolar o ponto de falha, buscar soluções alternativas até a resolução do problema, a fim de reduzir o impacto em todo o sistema (e seu consequente impacto no negócio) e reparar a falha. Existe um custo para se reparar e restaurar uma rede. Entre os impactos no negócio gerados pelas falhas da rede, pode-se citar o tempo desperdiçado, o dano à reputação e a perda de negócios existentes ou novos negócios. Uma rede lenta pode afetar o desempenho das aplicações e a produtividade da equipe. Uma rede de alto desempenho ajuda as empresas a lançarem seus serviços mais rapidamente, podendo melhorar o suporte através do aumento do tempo de atividade, do melhor desempenho das aplicações e da execução de aplicativos com segurança. Os desastres de rede e os custos de restauração podem ser evitados ou mitigados com o planejamento e suporte, além de manutenção proativa na rede. O processo de gerenciamento de falhas deve estar relacionado ao gerenciamento de serviços de rede e alinhado às necessidades do negócio. Como qualquer serviço de TI, os serviços de rede devem oferecer valor aos clientes (GOMEZ *et al*., 2017). Uma conexão efetiva entre a gestão de serviços de rede, elementos da rede, incidentes, falhas e negócio ainda é um desafio para os gestores.

Um domínio de alarme compreende três grupos de elementos: elementos iniciais, de passagem e finais. O fator determinante que discrimina em qual grupo de elementos pertence um componente de rede é a posição do nó de que faz parte dentro do canal. Os elementos de rede que fazem parte do grupo inicial são aqueles através dos quais o sinal óptico flui nos nós que estão no início do canal. Por sua vez, os elementos do grupo final são aqueles através dos quais o sinal óptico flui nos nós ao final do canal. Os elementos de rede pertencentes aos nós remanescentes do canal através dos quais o sinal óptico flui, que não estão nem no início nem no final do canal, caem no grupo de elementos passantes.

A técnica de redundância antecipada duplica componentes individuais, como linhas (tronco), redes de comutação, computadores de controle. No entanto, esta abordagem pode ter desvantagens em termos de viabilidade econômica. Para usar componentes simples e não redundantes de forma não estruturada, um nó redundante (SN1 ', SN2', SN3 ') logicamente idêntico é usado além de cada nó (SN1, SN2, SN3). Cada tronco (L1, L2, L3) entre nós também é complementado com um tronco redundante (L1 ', L2', L3 '), possivelmente conduzido através de um caminho físico diferente. Ambos os troncos estão conectados por meio de pelo menos um elemento combinador / divisor. Esta técnica é utilizada na rede de comunicação otimizada para redundância, para transmissão de sinais de comunicação (STEIN, 1999).

2.1.4.1 *Gerenciamento de Incidentes e Problemas*

O processo de gerenciamento de incidentes consiste em um dos processos importantes, recomendado pelo guia ITIL (OGC, 2007). Busca restaurar a operação normal do serviço o mais rápido possível e assim garantir os melhores níveis de qualidade e disponibilidade. Quando da implantação de melhores práticas, uma organização geralmente inicia a estruturação ou reestruturação de sua área de TI pelo processo de gerenciamento de incidentes, associado a uma função de *service desk* e ferramenta de *software* para controle dos incidentes. O gerenciamento de problemas é um processo que busca a resolução de incidentes que se repetem, e podem estar sendo gerado por problemas. Tem como objetivo a identificação e remoção de erros do ambiente de TI, através da busca da causa raiz dos incidentes registrados. Seu objetivo envolve análise de causalidade dos incidentes ocorridos na infraestrutura de TI, fornecendo soluções paliativas ou definitivas, que buscam evitar uma recorrência de incidentes, minimizando assim

o impacto desses incidentes. Um incidente não se torna um problema, mas pode estar relacionado a um. Enquanto o foco do processo de gerenciamento de problemas é resolver a causa dos incidentes, o foco do processo de gerenciamento de incidentes consiste no restabelecimento do serviço. São processos diferentes, porém complementares. As atividades básicas que envolvem os dois processos são similares, podendo-se citar a identificação, registro, classificação, priorização, investigação e diagnóstico, identificação de objetos conhecidos, resolução, encerramento e revisão dos objetos mais críticos.

A gestão de problemas pode ser *reativa*, quando busca proceder uma análise da causa dos principais incidentes ocorridos, visando resolver a causa e evitar a recorrência. Já a gestão de problemas *proativa* procede uma análise de informações dos itens de configuração (ICs), visando a identificação de oportunidades de melhoria, as quais podem ser registradas no plano de melhoria do serviço. Os métodos recomendados pelo ITIL para a análise e resolução de problemas possuem foco na área de qualidade. As principais saídas desse processo são as solicitações de mudanças para correção definitiva de problemas e incidentes relacionados. A mudança é autorizada ou não pelo *comitê de mudanças*, o qual avalia o custo das correções, o *impacto do problema* e as medidas de gestão envolvidas. No estabelecimento de prioridades, os gestores geralmente utilizam como critério decisório a combinação entre impacto e urgência do incidente/falha/problema. O alinhamento com negócio é um dos pontos essenciais a ser considerado nessas atividades.

Entre os problemas mais comuns relacionados ao gerenciamento de incidentes, destacam-se (O'CALLAGHAN, 2010):

- Falta de gestão ou comprometimento da equipe em relação aos incidentes;
- Falta de entendimento das necessidades do negócio para a priorização dos incidentes;
- Falta de objetivos, metas e responsabilidades no processo;
- Deficiência nos *Acordos de Nível de Serviços (SLAs)*, com possibilidade de geração de conflitos relativos à priorização;
- Falta de conhecimento técnico da equipe para solução dos incidentes;
- Falta de integração do processo com outros processos de gerenciamento de serviços;
- Falta de ferramentas de suporte para gestão dos incidentes;

- Resistência a mudanças em relação às regras do processo de gerenciamento de incidentes.

2.1.4.2 *Gerenciamento de Falhas*

Nas atividades de gerenciamento de redes de computadores, o processo de gerenciamento de falhas busca detectar, isolar, notificar e corrigir operações anormais no funcionamento dos recursos de rede.

De acordo com Specialski (2018), falhas não são o mesmo que erros. Uma falha é uma condição anormal cuja recuperação exige ação de gerenciamento e normalmente é causada por operações incorretas ou um número excessivo de erros. Caso uma linha de comunicação seja cortada fisicamente, nenhum sinal pode passar através da mesma. Um grampeamento no cabo pode causar distorções que induzem a uma alta taxa de erros. Certos erros como, por exemplo, um *bit* errado em uma linha de comunicação, podem ocorrer ocasionalmente e normalmente não são considerados falhas.

Para que exista o controle do sistema como um todo, cada componente crítico deve ser monitorado individualmente para garantir o seu perfeito funcionamento. Quando da ocorrência de uma falha, torna-se importante a possibilidade de uma ação rápida no sentido de determinar o componente exato onde a falha ocorreu; isolar a falha do resto da rede, para que ela continue a funcionar sem interferências; reconfigurar ou modificar a rede para minimizar o impacto da operação sem o componente que falhou; reparar ou trocar o componente com problemas para restaurar a rede ao seu estado anterior.

As responsabilidades envolvidas no gerenciamento de falhas incluem o monitoramento dos estados dos recursos da rede, a manutenção de cada um dos objetos gerenciados e as decisões que devem ser tomadas para restabelecer as unidades do sistema que possam apresentar problemas. Recomenda-se que as possíveis falhas sejam detectadas antes que os seus efeitos sejam percebidos.

O impacto e a duração do estado de falha podem ser minimizados pelo uso de componentes redundantes e rotas de comunicação alternativas, para dar à rede um maior grau de tolerância às falhas.

2.1.5 Geração de Valor

De acordo com Oliveira (2010), o alinhamento entre TI e o negócio vem repetidamente sendo apontado por pesquisas como um dos maiores desafios para a gestão de TI. Os guias de melhores práticas fornecem recomendações no sentido de associar os esforços da TI à geração de valor para o negócio, através de contribuições direcionadas ao cumprimento de seus objetivos estratégicos. A teoria sobre serviços fornece subsídios importantes para a modelagem do conceito de valor, de forma complementar aos clássicos da economia. As definições e classificações mais populares referentes a serviços oferecem *insights* interessantes para a representação mais formal do valor, embora possuam um elevado nível de subjetividade (OLIVEIRA, 2010).

Berry (1985) e Berry e Parasuraman (1991) produziram resultados consistentes no sentido de racionalizar o processo através do qual alguém atribui mais valor ou menos valor a um intangível. Dois elementos críticos que compõem o processo de criação da escala própria utilizada para qualificar tangíveis e intangíveis são apresentados: a expectativa e a percepção. Segundo Zeithaml *et al*., (1990), a qualidade de um serviço, construída através do aprimoramento de suas várias dimensões, é definida pela diferença existente entre as expectativas do receptor e a percepção que este tem do que lhe foi fornecido.

De acordo com a ISACA (2015), a criação de valor significa obter benefícios por meio da otimização do uso de recursos e dos riscos a um nível aceitável. Para cada parte interessada, a criação de valor pode representar interesses diferentes e algumas vezes conflitantes (Figura 4).

Figura 4. Objetivos da governança - Criação de valor. *Framework* do COBIT 5 (2015).

Como cada organização possui objetivos diferentes, o COBIT pode ser personalizado para o contexto da organização por meio da cascata de objetivos, ou seja, traduzindo os objetivos corporativos em alto nível em objetivos de TI específicos e gerenciáveis, mapeando-os em práticas e processos específicos. O sistema de governança abrange negociar e decidir entre os diferentes interesses dos *stakeholders* e deve considerar a opinião de todos quando são tomadas decisões sobre os benefícios, recursos e avaliação dos riscos. Para cada decisão de governança, questões podem e devem ser feitas:

- Quem recebe os benefícios?
- Quem assume os riscos?
- Quais são os recursos necessários?

Se não houver uma harmonia e equilíbrio entre esses três itens (benefícios, riscos e recursos), pode-se inferir que a gestão de TI não estará agregando valor.

2.2 GERENCIAMENTO DE RISCOS

Existem inúmeros fatores de risco que envolvem a atividade de gerenciamento de serviços de TI. Tais fatores são imprevisíveis e de difícil controle, como por exemplo as inovações tecnológicas, as mudanças constantes nos requisitos do cliente, falhas de equipamentos, parada de sistemas, dentre outros. As organizações precisam estar conscientes e gerenciar os riscos relacionados aos seus ativos vitais. Os gestores precisam planejar e se preparar para o provável e improvável (GÓMEZ *et al*., 2017).

Lidar com incertezas de mercado, inovações tecnológicas e aspectos regulatórios é parte inerente do setor de telecomunicações no Brasil. A gestão de riscos deve auxiliar o processo de decisão de forma a contribuir para o desempenho sustentável dos negócios e ter maior controle sobre perdas potenciais. O processo segue as etapas de identificação, avaliação e mitigação dos fatores internos e externos capazes de comprometer os objetivos e estratégias da organização.

Risco está relacionado à capacidade e continuidade operacional, principalmente de serviços críticos para os clientes, decorrentes de incidentes em *sites*, redes e torres, obsolescência ou falta de redundância de equipamentos, as quais podem gerar a indisponibilidade do serviço, perdas de equipamentos, danos a terceiros e lucros cessantes. O

monitoramento é feito por meio de processos, sistemas e indicadores do *Centro de Operações de Redes (COR)*, estrutura voltada para a detecção e tratamento dos incidentes. Os indicadores são reportados mensalmente à Anatel. Desde 2010, a companhia conta com um manual de crise, que prevê situações que podem comprometer a nossa reputação, como interrupção nos serviços, acidentes com associados e terceiros e greves. Em 2014, esse conteúdo foi aprimorado, com a criação de um plano de continuidade dos serviços de telecomunicações, visando prover uma direção para a governança e garantir a continuidade operacional e recuperação em casos de desastre.

Dada a dependência da nossa sociedade em infraestruturas de redes e a *Internet* em particular, pode-se afirmar que a resiliência deve ser uma propriedade integral das redes atuais e futuras. A gestão de riscos deve auxiliar o processo de tomada de decisão, a fim de contribuir para um desempenho empresarial sustentável e permitir um maior controle sobre potenciais perdas. O processo envolve os estágios de identificação, avaliação e mitigação de fatores internos e externos capazes de comprometer metas e estratégias corporativas. Cada risco deve ser gerenciado através do uso de metodologias, modelos de medição e controles específicos, gerando ações de mitigação que minimizem seus impactos no negócio.

De acordo com o PMI (2008), o gerenciamento de risco é uma das nove áreas de conhecimento existente no *Project Management Body of Knowledge (PMBOK)*. Consiste em um processo sistemático usado para identificar, analisar e responder aos riscos de um projeto, com o objetivo de maximizar a probabilidade dos eventos positivos e se possível neutralizar os eventos negativos ou minimizar suas consequências.

De acordo com a Norma ISO/IEC 27002 (ABNT, 2005), a análise de risco é utilizada na gestão de riscos em segurança da informação. O propósito de realizar uma análise de risco é para esclarecer se as ameaças são relevantes para os processos operacionais e identificar os riscos associados. Torna-se possível a identificação do nível de segurança adequado e medidas de segurança associadas. Uma análise de risco é utilizada para garantir que as medidas de segurança sejam implantadas em uma boa relação custo-efetivo, no momento oportuno e consequentemente, dar uma resposta eficaz às ameaças. A análise de risco ajuda a empresa a avaliar corretamente os riscos e determinar o correto equilíbrio das medidas de mitigação dos mesmos. Os gestores também podem analisar os custos envolvidos na tomada de cada medida preventiva ou corretiva. Uma análise de risco tem quatro objetivos principais:

1. Identificar os bens e os seus valores;
2. Determinar as vulnerabilidades e ameaças;
3. Determinar quais as ameaças se tornarão um risco e que podem interromper o processo operacional;
4. Determinar um equilíbrio entre os custos de um incidente e os custos de uma medida de segurança. Parte da análise de risco poder ser considerada uma análise custo / benefício.

Os custos periódicos associados às medidas de segurança são comparados com as perdas potenciais que poderiam ocorrer se as ameaças tornarem-se realidade. Deve-se evitar situações onde a prevenção é mais cara que o próprio ativo. Muitas vezes pode existir alguma dificuldade na estimativa do valor dos dados e das informações, como por exemplo, os danos à reputação da empresa causados por um incidente ou falha, como no caso de falhas associadas às redes ópticas.

Nóbrega *et al*., (2014) afirma que os objetivos do gerenciamento de riscos envolvem o aumento da probabilidade e do impacto dos efeitos positivos, com a redução da probabilidade e do impacto dos efeitos negativos. Busca-se identificar e priorizar os riscos de forma preventiva e fornecer informações orientadas a ações para os atores envolvidos no processo. Existem diversas ameaças e oportunidades que podem afetar de forma direta os serviços de tecnologia da informação. A própria característica inovadora de certas tecnologias e sua velocidade de atualizações requerem uma atenção redobrada dos gestores. A incidência de riscos existe durante todo o ciclo de vida de um serviço de TI. Obviamente, os riscos são quantificados e qualificados de forma diferente em cada momento do ciclo de vida de um serviço.

Entre as definições comuns de risco na literatura (NÓBREGA *et al*., 2014) cita:

i. a probabilidade de algo indesejável acontecer (um evento como uma falha na busca de um resultado, etc.);
ii. um valor de impacto esperado (a probabilidade de um evento multiplicado por seu impacto); e,
iii. uma medida da variabilidade dos resultados (esta é a abordagem utilizada no mundo financeiro).

Neste trabalho foi adotada a segunda definição de risco. Dessa forma, para os propósitos desta pesquisa, o risco decorre de um evento ou condição incerta que, se ocorrer, terá um impacto positivo ou negativo em algum atributo ou característica do objeto analisado, como tempo, custo, escopo ou qualidade. A análise de risco envolve, portanto, a avaliação da probabilidade de ocorrência de um evento e seu impacto relacionado. A avaliação do risco compara os níveis de risco com os critérios de risco estabelecidos. Avaliação de risco envolve os processos de análise de risco e avaliação de risco. Um relatório de análise de risco pode ser utilizado para alinhar os objetivos relacionados a TI com objetivos de negócios (GOMEZ *et al*., 2017). A Figura 5 apresenta a visão de Nóbrega *et al*., (2014) para o processo de gerenciamento de riscos em projetos de TI.

O gerenciamento de risco aborda situações que podem ser classificadas como oportunidades ou ameaças e que devem ser identificadas, analisadas, medidas e tratadas adequadamente, de acordo com a estratégia do negócio. A "medida de risco" está associada a cada situação. Os riscos devem ser priorizados antes que os planos de resposta sejam desenvolvidos. Um objetivo de gerenciamento de risco consiste em aumentar a probabilidade de impacto positivo, reduzindo a probabilidade de impacto negativo (NÓBREGA *et al*., 2014).

Na definição de risco adotada nesta pesquisa, a probabilidade é a "chance" da ocorrência de um risco, enquanto o impacto é a estimativa de "quanto" esse risco afetará o negócio. O valor de risco esperado (*Expected Risk Value - ERV*) é calculado multiplicando a probabilidade pelo impacto associado (*ERV = Probabilidade vs. Impacto*). Os riscos podem então ser classificados de acordo com seus *ERVs* e aqueles com maiores valores esperados devem ser tratados com maior prioridade.

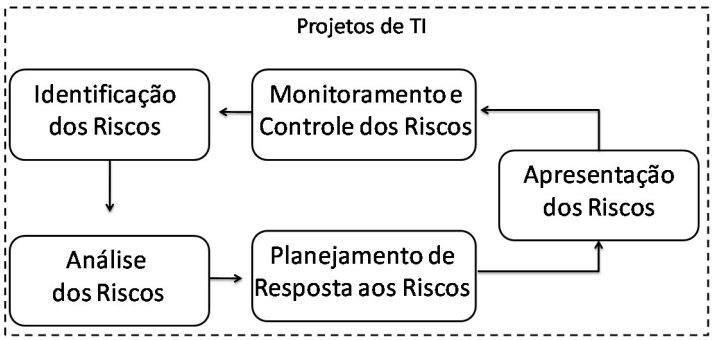


Figura 5. Método para gerenciamento de riscos. Nóbrega *et al*., (2014)

2.3 GESTÃO DE REDES

Quando módulos complexos de *hardware* e *software* que interagem uns com os outros são montados em conjunto, o sistema como um todo está vulnerável a defeitos. Existe a possibilidade que elementos da rede sejam mal configurados, que os recursos da rede sejam super utilizados ou que componentes da rede simplesmente sejam danificados (por exemplo, um cabo pode ser rompido). O operador de rede, cuja tarefa é manter esta operando quase que ininterruptamente, deve estar habilitado a reagir e a evitar esses problemas. Com milhares de componentes de rede espalhados por uma grande área, ele, em sua central de operações – *Centro de Gerência de Redes (CGR)*, necessita de ferramentas que o auxiliem a monitorar, administrar e controlar a rede. Para tanto, se faz necessário ter à mão as ferramentas de gerenciamento adequadas:

- Falha em uma placa de *interface* de um hospedeiro ou de um roteador. Com ferramentas de gerenciamento apropriadas, uma entidade de rede, por exemplo, um roteador, pode indicar ao operador de rede que uma de suas interfaces não está funcionando adequadamente. Um operador de rede que monitora e analisa de maneira ativa o tráfego da rede pode detectar problemas na interface antecipadamente e substituir a placa de interface antes que ela venha provocar algum tipo de falha.
- Monitoração de hospedeiro. O operador de rede pode verificar periodicamente se todos os hospedeiros da rede estão ativos e operacionais. Mais uma vez ele pode atuar, agindo pró-ativamente a um problema, por exemplo, falha em um hospedeiro, antes que a falha venha a ser percebida pelo usuário.
- Monitoração de tráfego para ajudar na utilização de recursos. Um operador de rede pode monitorar os padrões de tráfego entre fontes e destinos e notar, por exemplo, que trocando servidores entre segmentos de rede de área local, (*LAN-Local Area Network*), o total de tráfego inter-redes poderia ser reduzido de maneira significativa. De modo similar, monitorando a utilização de um enlace, um operador de rede pode determinar que um segmento de LAN ou um enlace para o mundo exterior está sobrecarregado e que um enlace de maior capacidade deve ser providenciado. Ele poderia ser notificado automaticamente quando o nível de congestionamento de um enlace ultrapassasse determinado limite, a fim

de fornecer um aumento da capacidade do enlace antes que o congestionamento venha a comprometer os serviços disponibilizados aos usuários da rede.

- Detecção de mudanças rápidas nas tabelas de roteamento. A alternância de rotas – mudanças frequentes nas tabelas de roteamento – pode indicar instabilidade no roteamento ou um roteador mal configurado. Evidentemente, um administrador de rede que configurou de modo inapropriado um roteador prefere ele mesmo descobrir o erro antes que ocorra algum tipo de evento na rede.
- Monitoração de SLA's. Com o advento dos SLA's (*Service Level Agreements*) - contratos que definem parâmetros específicos de medida e níveis aceitáveis de desempenho do provedor de rede em relação a essas medidas - o interesse na monitoração do tráfego cresceu significativamente nos últimos anos. O UNet e o AT&T (*American Telephone and Telegraph*) são apenas dois dos muitos provedores de rede que garantem os SLA's a seus usuários. Dentre esses SLA's destacam-se a disponibilidade de serviço (interrupção de serviços), a latência, a vazão e as exigências quanto à notificação da ocorrência "serviço interrompido". É claro que, se critérios de desempenho fizerem parte dos contratos de prestação de serviços entre um provedor de rede e seus usuários, então a medição e o gerenciamento do desempenho do sistema também serão de grande importância para o administrador de rede.
- Detecção de intrusos. Um operador de rede provavelmente vai querer ser avisado quando chegar um tráfego de uma fonte suspeita ou quando se destinar tráfego a ela. Semelhantemente, ele pode querer detectar e filtrar a existência de determinados tipos de tráfego que são indicativos da presença de intrusos na rede.

2.3.1 Gerenciamento de redes de telecomunicações

O ITU-T começou a padronização das redes de gerência de telecomunicações, denominada como TMN (ITU-T M.3010, 2000)(JAMES, 1987), em 1985, para possibilitar que

redes de gerência sejam implementadas a partir de sistemas de diferentes fabricantes. A sustentação das necessidades de gerência de uma empresa de telecomunicações é dada pelo modelo de referência TMN, fazendo que a empresa planeje, instale, administre as redes e os serviços de telecomunicações.

A planta de telecomunicações é composta de elementos de rede (equipamento que se comunica com a TMN, segundo padrões do ITU-T, com o intuito de ser monitorado e/ou controlado (ITU-T ,2000)) de diferentes fabricantes, e de sistemas de suporte à operação (programa que processa informações relacionadas à gerência de telecomunicações, com o objetivo de monitorar, coordenar e/ou controlar as funções de telecomunicações (ITU-T, 2000)).Devido aos blocos funcionais serem de diferentes fabricantes, a padronização da TMN baseia-se na ideia de pontos de referência, que atuam como delimitadores entre os blocos funcionais e possuem o objetivo de identificar os dados permutados entre os blocos. Para efeito de implementação, normalmente, cada ponto de referência indica uma interface entre dois blocos.

O ITU-T em conjunto com a ISO (International Organization for Standartization), criou padrões não só para protocolos, mas também para os modelos de informações a serem adotados na comunicação, tudo isso com o objetivo de permitir o intercâmbio de informações através das interfaces.

A edição de uma lista de recomendações foi o resultado do esforço realizado pelo ITU-T. Uma visão global dos padrões do ITU-T no que diz respeito a TMN, pode ser visto em (ITU-T M3000, 1994). A arquitetura TMN, abrangendo os aspectos referentes à troca de dados entre os elementos da rede e os aspectos físicos e funcionais, pode ser encontrado em (ITU-T M3010, 2000).

Atualmente, devido à digitalização da rede e à inteligência dos elementos que a compõem, a TMN é uma das peças fundamentais da gerência das redes de telecomunicações, não somente pelas qualidades de elegância conceitual, mas também pela robustez e consistência (Meira, 1997).

2.3.2 Gerência no modelo OSI

O sistema representa os recursos gerenciados através de entidades lógicas chamadas de objetos gerenciados. Ao desenvolver uma aplicação de gerenciamento, usam-se processos distribuídos conhecidos como gerentes (os quais gerenciam) e agentes (os quais realizam as ações) (SZTANJNBERG, 2004).

Além de definir um modelo informacional, define-se também um modelo funcional em que, para cada área é definido um conjunto de funções que ao serem implementadas serão usadas para gerenciar a rede.

O campo de gerenciamento de rede tem sua terminologia específica para os vários componentes da arquitetura de gerenciamento de rede; Na Figura 6 pode-se observar os principais componentes de uma arquitetura de gerenciamento de rede: uma entidade gerenciadora, os dispositivos gerenciados e um protocolo de gerenciamento de rede.

A entidade gerenciadora é uma aplicação que em geral tem um ser humano no circuito e que é executada em uma estação central de gerência de rede no CGR. Ela é o *locus* da atividade de gerenciamento de rede, ela controla: a coleta, o processamento, a análise e/ou a apresentação de informações de gerenciamento de rede. É nela que são iniciadas as ações para controlar o comportamento da rede e que o administrador humano interage com os dispositivos da rede (SZTANJNBERG, 2004).

O dispositivo gerenciado é um equipamento residente em uma rede gerenciada e pode ser um hospedeiro ou um roteador. No interior de um dispositivo podem haver diversos objetos gerenciados. Estes são, na verdade, as peças de hardware que estão dentro do dispositivo gerenciado, por exemplo, uma placa de interface de rede e/ou os conjuntos de parâmetros de configuração para as peças de hardware e software, por exemplo, um protocolo de roteamento intradomínio, como o Protocolo de Roteamento de Informações, RIP (*Routing Information Protocol*). Esses objetos gerenciados têm informações associadas a eles que são coletadas dentro da Base de Informações de Gerenciamento, MIB (*Management Information Base*). Em cada dispositivo gerenciado reside um agente de gerenciamento de rede, um processo que é executado no dispositivo gerenciado, que se comunica com a entidade gerenciadora.

O terceiro componente de uma arquitetura de gerenciamento de rede é o protocolo de gerenciamento de rede. Esse protocolo é executado entre a entidade gerenciadora e o agente de gerenciamento de rede dos dispositivos gerenciados, o que permite que a primeira investigue o estado dos dispositivos gerenciados e, indiretamente, execute ações sobre eles mediante seus

agentes. Os agentes podem usar o protocolo de gerenciamento de rede para informar à entidade gerenciadora a ocorrência de eventos excepcionais, por exemplo, falhas de componentes ou violação de patamares de desempenho.

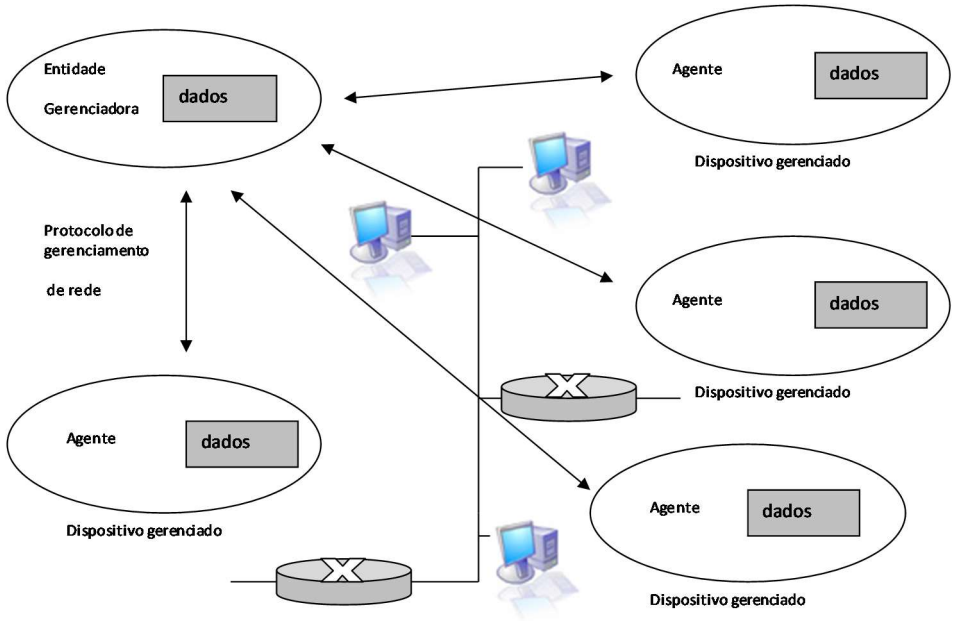


Figura 6. Principais componentes de uma arquitetura de gerenciamento de rede. Sztanjnberg (2004).

É importante notar que o protocolo de gerenciamento de rede em si não gerencia a rede. Em vez disso, ele fornece uma ferramenta com a qual o operador de rede pode gerenciar, monitorar, testar, consultar e controlar a rede.

2.3.2.1 Modelo de gerenciamento OSI

O modelo de gerenciamento OSI está definido com base nos conceitos abaixo:

- Considerando-se a estrutura de gerenciamento;
- Considerando-se as MIBs;

Na estrutura de gerenciamento têm-se três tipos de gerenciamento (SZTANJNBERG, 2004):

- Gerenciamento de sistemas: é um protocolo executado na camada de aplicação que é responsável pelo gerenciamento dos sistemas. Pode-se gerenciar aqui quaisquer objetos associados a um sistema aberto. Este gerenciamento necessita do apoio das funções de todas as sete camadas do modelo OSI para poder realizar o gerenciamento;
- Gerenciamento de camada: Este gerenciamento é realizado sobre os objetos gerenciados, relacionados às atividades de uma camada particular. O gerenciamento de camada usa os protocolos de gerenciamento de propósito especial que não prestam serviços às camadas superiores, e são independentes dos protocolos de gerenciamento das outras camadas.
- Operação de camada: É usada no gerenciamento de uma única instância de comunicação em uma camada. É um tipo de gerência que exige menores requisitos das funções de apoio, por não ser necessário um protocolo particular para a troca de informações de gerenciamento, pois utiliza o protocolo normal da camada para trocar estas informações.

Normalmente, os dados utilizados em sistemas complexos são armazenados em algum tipo de base de dados. Esta base de dados é a MIB. Uma MIB é usada para armazenar as informações transferidas ou modificadas quando são usados os protocolos de gerenciamento OSI. As informações podem ser fornecidas por agentes administrativos locais ou por sistemas abertos remotos. Uma interface específica para cada camada é obtida através das Entidades de Gerenciamento de Camadas, LME (Layer Management Entities). Cada LME contém a funcionalidade da camada a que está relacionada. A integração destas entidades e a execução da função de interfaceamento com gerente são executadas pela Entidade de Aplicação da Gerência de Sistemas SMAE (System Management Application Entity). Esta entidade também providência a interface entre as LMEs de um nó da rede com as suas correspondentes no outro nó, usando o protocolo de informação de gerenciamento. Na Figura 7 pode-se visualizar o modelo de gerenciamento OSI.

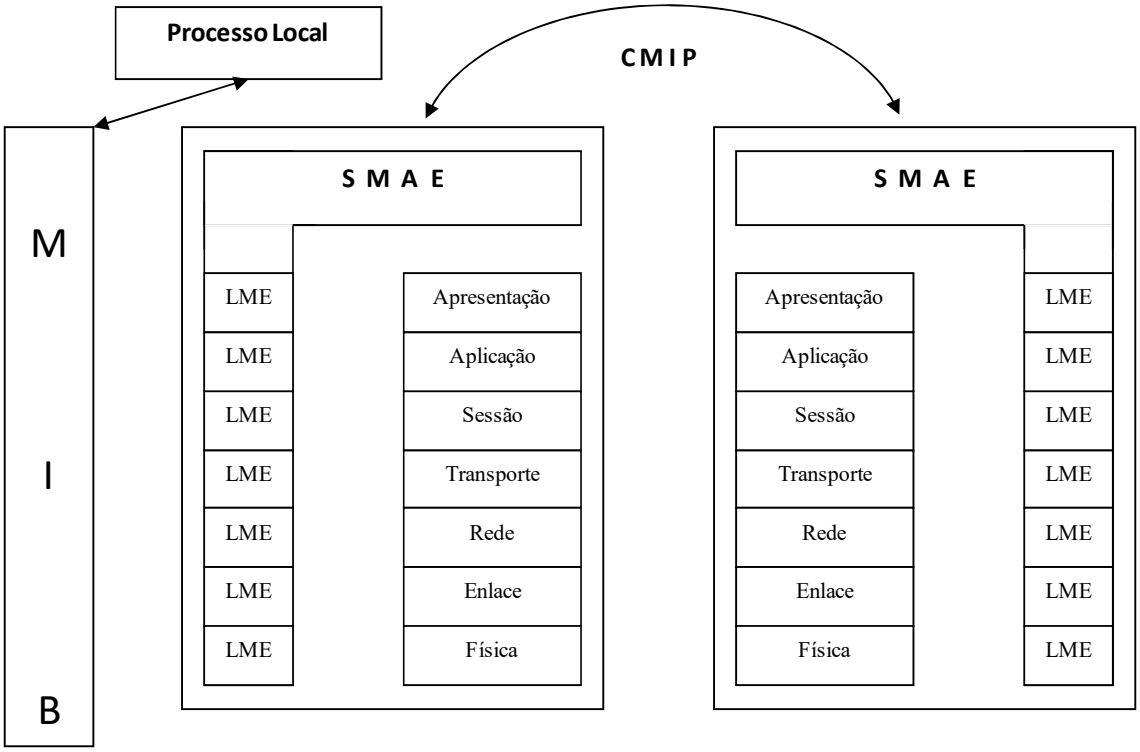


Figura 7. Modelo de Gerenciamento OSI. Sztanjnberg (2004)

Deve-se agrupar em unidades funcionais todos os serviços fornecidos por alguma função de gerenciamento de sistema. Estas unidades são básicas para a negociação entre os Serviços de Informação da Gerência – Usuários, MIS-Users (*Management Information Service - Users*), que são aplicações que utilizam os serviços de gerenciamento e que podem desempenhar tanto a função de um agente como a de um gerente. Quando tem a função de agente, o MIS-Users é parte de alguma aplicação distribuída que controla os objetos gerenciados no seu domínio (ambiente local) e realiza operações sobre os objetos gerenciados em função dos comandos enviados pelo gerente, podendo também enviar notificações dos objetos gerenciados aos gerentes.

2.3.2.2 Componentes do modelo de gerenciamento OSI

Como o ambiente a ser gerenciado é distribuído, as atividades de gerência também devem ser distribuídas. Uma instância de uma aplicação distribuída pode ser formada por uma associação de duas ou mais aplicações de gerenciamento do sistema.

As interações entre os sistemas são feitas através das operações de gerenciamento e das notificações, sendo que uma entidade tem a função de um gerente, solicitando ações de gerenciamento à outra entidade que tem a função de agente, executando as operações e enviando as notificações emitidas pelos objetos gerenciados.

Um pedido de operação que chega a um agente é rejeitado, a menos que os mecanismos que controlam os acessos aos objetos gerenciados permitam ao gerente realizar as operações solicitadas sobre estes objetos. Sempre que existam notificações a serem enviadas pelos objetos gerenciados, o sistema gerenciado (agente) envia tais notificações aos gerentes.

Para a execução das atividades acima dois aspectos são necessários na comunicação:

- Suporte para a transferência dos pedidos de operações de gerenciamento e para o envio de notificações entre MIS-Users;
- Suporte para controle de acesso dos objetos gerenciados e para a distribuição das informações das notificações.

AISO criou um modelo de gerenciamento de rede que é útil para situar os cenários apresentados em um quadro mais estruturado. São definidas cinco áreas de gerenciamento de rede:

- Gerenciamento de desempenho. A meta do gerenciamento de desempenho é quantificar, medir, analisar e controlar o desempenho (por exemplo, utilização e vazão) dos diferentes componentes da rede. Entre esses componentes estão os dispositivos individuais (por exemplo, enlaces, roteadores e hospedeiros) bem como abstrações fim a fim (como um trajeto pela rede).
- Gerenciamento de falhas. O objetivo do gerenciamento de falhas é registrar, detectar e reagir às condições de falha da rede. A linha divisória entre gerenciamento de falha e gerenciamento de desempenho é bastante tênue. Pode-se considerar o gerenciamento de falha como algo mais restrito, como o tratamento imediato às falhas que causam descontinuidade dos serviços da rede,

por exemplo, interrupção de serviço em enlaces, hospedeiros ou em hardware e software e/ou roteadores. O gerenciamento de desempenho, por sua vez, pode ser visto de maneira mais ampla, como o fornecimento de níveis aceitáveis de desempenho em face de demandas variáveis e de ocasionais falhas de rede. Como acontece no gerenciamento de desempenho, o SNMP tem um papel fundamental no gerenciamento de falhas.

- Gerenciamento de configuração. O objetivo da gerência de configuração é o de estabelecer parâmetros de operação de rede, coleta de informações sobre a configuração atual da rede, alteração da configuração da rede, por exemplo, ativando ou desativando componentes da mesma, armazenamento de informações relativas à configuração da rede e emissão de relatórios baseados nas mesmas. A gerência de configuração, portanto, é correspondente a um conjunto de facilidades que permitem controlar os objetos gerenciados, identificá-los, coletar e disponibilizar dados sobre estes objetos para as seguintes funções:
  i. Atribuição de valores iniciais aos parâmetros de um sistema aberto;
  ii. Início e encerramento das operações sobre objetos gerenciados;
  iii. Alteração da configuração do sistema aberto;
  iv. Associação de nomes a conjuntos de objetos gerenciados.
- Gerenciamento de contabilização. O gerenciamento de contabilização permite que o operador da rede especifique, registre e controle o acesso de usuários e dispositivos aos recursos da rede. A coleta de dados sobre a utilização dos recursos de rede, o estabelecimento de quotas de utilização de tais recursos vinculadas a usuários ou grupos de usuários, o estabelecimento de escalas de tarifação associadas ao uso desses recursos, a determinação dos custos envolvidos, realizando a combinação de custos quando múltiplos recursos são utilizados dentro de um dado objetivo de comunicação e a emissão de relatórios sobre a utilização dos recursos de rede e os custos correspondentes fazem parte do gerenciamento de contabilização.
- Gerenciamento de segurança. A meta do gerenciamento de segurança é controlar o acesso aos recursos da rede de acordo com alguma política definida. As centrais de distribuição de chaves e as autoridades certificadoras são componentes do gerenciamento de segurança. O uso de programas específicos

de segurança para monitorar e controlar pontos externos de acesso à rede é outro componente crucial.

Após as explanações anteriores, pode-se definir gerenciamento de rede em uma única sentença dada por Saydam (MEIRA, 1997):

"*Gerenciamento de rede inclui a disponibilização, a integração e a coordenação de elementos de hardware, software e humanos, para monitorar, testar, consultar, configurar, analisar, avaliar e controlar os recursos da rede e de elementos, para satisfazer às exigências operacionais, de desempenho e de qualidade de serviço em tempo real a um custo razoável".*

2.3.2.3 Gerência na Internet

Ao contrário do que o nome SNMP possa sugerir, o gerenciamento de rede na *Internet* deixou de ser apenas um protocolo para transportar dados de gerenciamento entre uma entidade gerenciadora e seus agentes. O SNMP passou a ser mais complexo do que o nome "simples" possa sugerir. As raízes da atual estrutura de gerenciamento de rede da Internet reportam ao protocolo de monitoração de passagem simples, SGMP (*Simple Gateway Monitoring Protocol*).

Na descrição de qualquer estrutura para gerenciamento de rede, certas questões devem inevitavelmente ser abordadas:

- O que está sendo monitorado? E que tipo de controle pode ser exercido pelo operador de rede?
- Qual é o modelo específico das informações que serão relatadas e/ou permutadas?
- Qual é o protocolo de comunicação para a troca de informações?

A estrutura de gerenciamento de rede da Internet aborda essas questões. A estrutura é constituída de quatro partes:

- Definições dos objetos de gerenciamento de rede, conhecidos como objetos MIB. Na estrutura de gerenciamento de rede da internet, as informações de gerenciamento são representadas como uma coletânea de objetos gerenciados que, juntos, formam um banco de informações conhecido como MIB. Um objeto MIB pode ser um contador, como o número de datagramas IP descartados em um roteador devido a erros nos cabeçalhos do datagrama IP ou o número de erros

de detecção de portadora em uma placa de interface Ethernet; ele pode ser um conjunto de informações descritivas, como a versão do software que está sendo executado em um servidor do Sistema de Nomeação de Domínio, DNS (*Domain Naming System*), informações de estado, como se um determinado dispositivo está funcionando corretamente ou não, ou informações específicas sobre protocolos, como um caminho de roteamento até um destino. Assim, os objetos MIB relacionados são colocados dentro de módulos MIB.

- Uma instrumentação de gerenciamento, conhecida como Estrutura de Gerenciamento de Informações, SMI (*Structure of Management Information*), que define os tipos de dados, um modelo de objeto e as regras para escrever e revisar informações de gerenciamento. A SMI é a estrutura de dados de gerenciamento. Ela é especificada em ASN.1, linguagem para especificação abstrata de dados. Os objetos MIB são especificados nessa instrumentação.
- Um protocolo, o SNMP, para transportar as informações e os comandos entre uma entidade gerenciadora e um agente que os executa, em nome da entidade, dentro de um dispositivo de rede gerenciado.

Assim, a arquitetura de gerenciamento de rede da Internet é modular por projeto, com uma linguagem de definição de dados independente de protocolo e um protocolo independente de MIB. A seguir examinar-se-á com mais detalhes os quatros componentes mais importantes da estrutura de gerenciamento de rede da internet.

- SMI - É a estrutura de dados usada para definir as informações de gerenciamento que residem em uma entidade de rede gerenciada. Essa linguagem de definição é necessária para assegurar que a sintaxe e a semântica dos dados de gerenciamento de rede sejam bem definidas e não apresentem ambiguidade. Note que a SMI não define um exemplar específico para os dados em uma entidade de rede gerenciada, mas a linguagem na qual a informação está especificada.
- MIB - A MIB pode ser vista como um banco de informações que guarda objetos gerenciados, cujos valores, coletivamente, refletem o status atual da rede. Esses valores podem ser pesquisados e/ou definidos por uma entidade gerenciadora, por meio do envio de mensagens SNMP ao agente que está executando em um nó gerenciado em nome da entidade gerenciadora. Os objetos gerenciados são especificados com o uso da construção OBJECT-TYPE (usada para especificar o

tipo de dado, o status e a semântica de um objeto gerenciado) e agrupados em módulos MIB que utilizam a construção MODULE-IDENTITY (permite que os objetos relacionados entre si sejam agrupados, como conjunto dentro de um módulo).

- Operações do protocolo SNMP e mapeamentos de transporte - O SNMPv2 é usado para transportar informações da MIB entre entidades gerenciadoras e agentes, executando em nome das entidades gerenciadoras. O uso mais comum do SNMP é desenvolvido no modo comando-resposta, no qual a entidade gerenciadora SNMPv2 envia uma requisição a um agente SNMPv2, que a recebe, realiza alguma ação e envia uma resposta à requisição. Em geral, uma requisição é usada para consultar ou modificar valores de objetos MIB associados ao dispositivo gerenciado. Um segundo uso comum do SNMP é para um agente enviar uma mensagem não solicitada, conhecida como mensagem *trap*, à entidade gerenciadora. As mensagens *trap* são usadas para notificar uma entidade gerenciadora de uma situação excepcional que resultou em mudança nos valores dos objetos da MIB. O operador de rede pode requerer uma mensagem de *trap*, por exemplo, quando uma interface cai, quando o congestionamento atinge um nível predefinido ou quando ocorre qualquer outro evento notável.
- Segurança e Administração - Os projetistas do SNMPv3 têm dito que "o SNMPv3 pode ser pensado como um SNMPv2 com capacidades adicionais de segurança e de administração", (SZTANJNBERG, 2004). Certamente, há mudanças no SNMPv3 em relação ao SNMPv2, mas em nenhum lugar essas mudanças são mais evidentes do que nas áreas da administração e da segurança. O papel central da segurança no SNMPv3 é muito importante, já que a falta de segurança adequada resultava no uso do SNMP, primordialmente, para monitorar, em vez de controlar. As denominadas aplicações SNMP consistem em um gerador de comandos, um receptor de notificações e um transmissor *Proxy*, todos normalmente encontrados em uma entidade gerenciadora; um elemento que responde os comandos e um que é responsável pela origem de notificações, ambos tipicamente encontrados em um agente, e na possibilidade de outras aplicações. Foi visto, anteriormente, que as mensagens SNMP são usadas não somente para monitorar, mas também para controlar elementos da rede. É claro que um intruso que conseguisse interceptar mensagens SNMP e/ou gerar seus próprios pacotes SNMP na infraestrutura de

gerenciamento poderia criar um grande tumulto na rede. Assim, é crucial que as mensagens SNMP sejam transmitidas com segurança. Surpreendentemente, foi somente na versão mais recente do SNMP que a segurança recebeu a atenção merecida. O SNMPv3 fornece criptografia, autenticação, proteção contra ataques de reprodução e controle de acesso. Sua segurança é conhecida como segurança baseada no usuário, pois utiliza o conceito tradicional de um usuário, identificado por um nome de usuário, ao qual as informações de segurança uma senha, um valor de chave ou acessos privilegiados – são associados.

2.3.2.4 Gerência de falhas

Uma das áreas mais importantes na gerência de redes de telecomunicações consiste da gerência das falhas ocorridas durante o funcionamento dessas redes. Segundo o ITU-T, gerência de falhas engloba detecção, isolação e correção de falhas (ITU-T X700, 1992). O processo que identifica as falhas em um grande sistema de comunicações é dividido em detecção, localização e identificação:

- Detecção da falha: A detecção da falha pode ser através de uma indicação de uma conexão em tempo real, que demonstra que algum componente da rede não está funcionando corretamente. Normalmente, os elementos das redes de comunicação providenciam indicações na forma de alarmes, quando eles não estão funcionando corretamente. Assim, a detecção de falhas pode ser providenciada pelos elementos da rede.
- Localização da falha: É a análise dos alarmes dos dispositivos da rede, a fim de indicar uma possível hipótese das falhas. Este passo é essencial, visto que, na maioria dos casos, os alarmes não mostram ou não detalham a identificação do elemento que está em mau funcionamento, pois os alarmes trazem de fato, a identificação de quem está enviando o alarme.
- Identificação da falha: A falha vigente é isolada, dado um número de possíveis hipóteses de falhas. Testes de acesso e de equipamentos devem ser o caminho mais apropriado para o isolamento da falha neste estágio.

Para uma planta de telecomunicações típica, o problema relacionado à carência de informações no centro de gerência de rede está gradativamente perdendo relevância. De fato, o

crescimento da planta gerenciada, associado à implantação de modernos sistemas de gerência, está criando um grande aumento no volume de informações recebidas nos centros de gerência, tornado praticamente inviável o processamento manual de todas elas (ITU-T G709, 2003).

As ferramentas de gerenciamento podem auxiliar no processo de análise de falhas de acordo com a seguinte sequência (HICORP, 2002):

- Identificação dos problemas – um dos grandes desafios dos sistemas de gerenciamento é a identificação de uma anormalidade antes do recebimento da notificação por parte do usuário, tarefa extremamente difícil de ser executada. A crescente demanda do mercado por soluções que ofereçam maior auxílio fez com que fossem desenvolvidos aplicativos capazes de monitorar serviços ou aplicações. Alguns dos métodos utilizados para a identificação de anormalidades são:
  - Chamada: coleta de dados em intervalos periódicos para análise futura.
  - Notificação: informação enviada pelo agente SNMP do objeto, indicando a ocorrência de um evento.
  - Limiar: configuração de limites de monitoração
- Correlação de alarmes – após ter definido quais mecanismos serão utilizados para a identificação das falhas, é importante estabelecer um mecanismo de controle dos eventos sinalizados. Isto se faz necessário, pois a administração destes eventos não é uma tarefa fácil de ser desenvolvida, uma vez que um evento de falha pode ser sinalizado por diversos elementos da rede dificultando o tratamento do problema. O operador da rede deve possuir ferramentas que o auxiliem no processo de tratamento das falhas, agrupando eventos que se referem ao mesmo problema e otimizando o Tempo de Reparo Médio, MTTR (*Mean Time to Repair*) (HICORP, 2002).
- Isolamento e resolução – o conhecimento necessário para a identificação e resolução de anormalidades é diretamente proporcional à complexidade do problema. Embora as ferramentas de gerenciamento tenham evoluído na apresentação ou tentativa de identificação de irregularidades, a maior parte da tarefa continua sendo do operador da rede. Este processo pode ser observado até mesmo em outras áreas de conhecimento como, por exemplo, a medicina. Equipamentos e sistemas de análise médica coletam e analisam as mais diversas informações. A conclusão ou diagnóstico final porém, ainda envolve decisões humanas. Mesmo com o auxílio de ferramentas de gerenciamento não há como gerenciar uma rede em sua totalidade

sem ter o conhecimento das tecnologias empregadas, do comportamento dos elementos monitorados e das aplicações dos usuários (HICORP, 2002).

- Testes e documentação – antes de assumir como definitiva qualquer solução, são necessários testes para a verificação das funcionalidades afetadas, bem como a análise criteriosa com o objetivo de garantir que nenhum outro elemento ou sistema será prejudicado com as alterações propostas. A documentação também é um processo de extrema relevância, sobretudo para incrementar a base de dados de conhecimento que algumas aplicações disponibilizam a fim de facilitar análises futuras, diminuindo o MTTR, pois com a base de dados, se uma falha voltar a ocorrer, os efeitos da mesma estarão na base de dados e rapidamente a falha será identificada, diminuindo desta forma o MTTR (HICORP, 2002).

Algumas ferramentas de gerenciamento permitem, através de processos de documentação, que sejam elaborados históricos para análise de problemas, facilitando o processo de procura de falhas.

Wang *et al*., (2014) apresentaram um método de monitoramento de desempenho e previsão de falhas em redes ópticas baseadas em aprendizado de máquina, utilizando os algoritmos máquina de vetores de suporte (*SVM*) e suavização exponencial dupla (*DES*). Segundo os autores, o método *DES-SVM* pode efetivamente melhorar os modelos tradicionais de risco para proteger os serviços de possíveis falhas e melhorar a estabilidade da rede óptica. O método de predição proposto apresentou alta precisão (95%) na predição de falhas de equipamentos ópticos, podendo prever falhas da placa em uma rede *WDM*, o que significa que os serviços podem ser protegidos contra perda de dados antes que ocorra uma falha na rede. A solução proposta depende de dados da rede, e apresentou baixo desempenho em períodos onde sua tendência mudou notavelmente, fato que não inviabiliza sua aplicabilidade.

2.3.3 Correlação de diagnóstico de falhas

2.3.3.1 Correlação de alarmes

Um objeto gerenciado é definido como uma visão de um recurso da rede de telecomunicações, sob o ponto de vista do sistema de gerência (ITU-T X700, 1992). Contudo,

sob o ponto de vista de correlação de alarmes - a representação de um recurso real que pode enviar alarmes em resposta ao surgimento de algum evento interno a ele, é denominada de objeto gerenciado. Não tão somente os alarmes, mas também os dados que eles contêm, são definidos pela classe de objetos gerenciados da qual o objeto gerenciado é uma instância (ITU-T X700, 1992).

A falha é conceituada como o motivo de um mau funcionamento no contexto de gerência de redes. Elas dificultam e impedem que os sistemas funcionem adequadamente, fazendo que estes apresentem erros (MEIRA, 1997).

A notificação sobre a ocorrência de um evento específico, que pode ou não representar um erro, é definida como alarme. O transporte dos dados dos alarmes é feito pelo relatório de alarme, que é um tipo de relatório de evento (utilizados para, através do uso de protocolos de comunicação, reportar a ocorrência de eventos em um objeto gerenciado (ITU-T X710, 1991)).

A correlação como uma técnica que origina uma quantidade mínima de hipóteses de falhas para um certo número de alarmes é a visão de autores como Hopfmuller (KEHL e HOPFMULLER, 1993). Contudo, autores como Jakobson, (JAKOBSON e WEISSMAN, 1995) consideram que a correlação de alarmes consiste na interpretação conceitual de múltiplos alarmes, levando à atribuição de um novo significado aos alarmes originais. A primeira definição é adequada para o contexto de diagnóstico de falhas, pois é uma das etapas do processo de gerência de falhas que consiste em descobrir qual a causa original dos alarmes recebidos. Todavia, um alarme nem sempre está associado a uma falha, então o segundo conceito deve ser empregado.

A correlação de alarmes pode ser aplicada a qualquer das cinco áreas funcionais de gerência definidas pelo ITU-T, quais sejam: falhas, configuração, contabilização, desempenho e segurança (ITU-T X700, 1992).

Numa empresa de médio porte o centro de gerência poderá receber dezenas de milhares de alarmes por dia. Segundo (HOUCKS, *et al.,*1995) são vários os motivos que levam a isso:

- Uma única falha em um elemento de rede pode provocar a emissão de múltiplos alarmes, pois o mesmo pode pertencer a vários canais e uma falha nele implicará na interrupção dos canais aos quais ele faz parte, como por exemplo: a fibra ou o multiplexador;
- O envio de um mesmo alarme pode ocorrer repetidas vezes, quando da ocorrência de uma falha intermitente, como por exemplo, um cabo de fibra aéreo submetido a

um grande esforço mecânico que a mínima oscilação da posteação provoca um mau contato nos conectores;

- ❖ Se um elemento de rede está funcionando inadequadamente, toda vez que for necessário a utilização de algum serviço deste haverá a emissão de alarme, como por exemplo, quando o comutador de proteção for solicitado e ele estiver defeituoso(s) alarme(s) será(ão) enviados para a gerência;
- ❖ O mesmo alarme será emitido repetidas vezes, caso a falha que o originou seja detectada por múltiplos elementos de rede;
- ❖ Se uma falha pertinente a um elemento de rede afetar outros elementos, a mesma poderá se propagar.

Em vista da facilidade de acesso aos mais diversos recursos computacionais, fazer a correlação de alarmes manualmente não é muito eficiente. Uma correlação de alarmes automática provê uma maior facilidade de acesso às informações e uma maior rapidez e eficiência em todo o processo de diagnóstico de falhas.

2.3.3.2 Tipos de correlação

De acordo com a técnica empregada sobre os alarmes, diferentes tipos de correlação podem ser identificados (JAKOBSON e WEISSMAN, 1995). As técnicas de correlação mais conhecidas são: compressão, supressão seletiva, filtragem, contagem, escalação, generalização, especialização, relacionamento temporal e aglutinação.

Características como as arquiteturas das redes de telecomunicações gerenciadas e da rede de gerência, bem como os objetivos da correlação devem ser considerados durante a escolha do sistema de correlação.

Inicialmente, além de identificar quais as áreas funcionais a serem servidas pela correlação de alarmes, é importante caracterizar o objetivo da correlação, o qual pode incluir desde a redução do volume de informações encaminhadas aos gerentes de redes até algo mais elaborado, tal como a localização e o diagnóstico de falhas ou a predição do comportamento futuro da rede baseada em análise de tendências (MEIRA, 1997).

A topologia do sistema de correlação deverá ser especificada logo que os objetivos da correlação forem determinados, para que sejam definidos onde ficarão os dispositivos correlatores e que tipo de relação deve existir entre eles.

A correlação pode ser realizada tanto em nível de elemento de rede isolado quanto em nível de componente de elemento da rede, dependendo do grau de configuração. Processos menos complexos e mais rápidos ocorrem quando há correlação em níveis mais baixos. Todavia, este tipo de correlação tem problemas quando se trata de falhas locais que interferem em toda a rede. No outro extremo, quando se trabalha com correlação em nível mais alto, este tipo de problema não existe, pois todos os dados relevantes são enviados para serem correlacionados. No entanto, o excesso de dados a serem trabalhados torna o processo bastante complexo e difícil de operar.

A quantidade de técnicas utilizadas para a correlação cresceu significativamente. Algumas dessas abordagens são probabilísticas, outras utilizam paradigmas tradicionais de inteligência artificial (IA) e outras tantas aplicam princípios definidos em lógicas não-convencionais (SMETS, *et al.*, 1988).

Dentre as mais importantes técnicas para a correlação de alarmes para redes de telecomunicações podemos destacar os seguintes métodos e algoritmos utilizados no processo de correlação (MEIRA, 1997):

- Correlação baseada em regras;
- Correlação utilizando lógica difusa;
- Redes bayesianas ou redes causais;
- Raciocínio baseado em modelos;
- Quadro-negro;
- Filtragem;
- Descriminador do Remessa de Evento, EFD (Event Forwarding Discriminator);
- Raciocínio baseado em casos;
- Correlação por codificação;
- Correlação por localização explícita;
- Correlação por votação;
- Correlação proativa;
- Correlação distribuída;

- ❖ Correlação distribuída baseada em serviço;
- ❖ Correlação distribuída baseada em políticas;
- ❖ Redes neurais artificiais;
- ❖ Diagnóstico por comparação de resultados;
- ❖ Análise de causa raiz;
- ❖ Correlação utilizando mineração de eventos;
- ❖ Correlação baseada no modelo transversal;
- ❖ Correlação canônica;
- ❖ Raciocínio hierárquico;
- ❖ Correlação baseada na representação formal de dependências;
- ❖ Redes de Petri.

A princípio, qualquer uma das abordagens citadas acima poderia ter sido escolhida, pois cada uma delas possui vantagens e desvantagens. Visando obter uma abordagem mais eficiente, foi adotado um modelo formado pela coesão de diferentes técnicas que deve atender as seguintes características: facilidade de construção, habilidade de trabalhar com informações incompletas, filtragem inteligente e facilidade de implementação de esquemas de localização de falhas.

As abordagens utilizadas para a criação do modelo desenvolvido neste trabalho estão enumeradas logo a seguir:

1. Correlação baseadas em regras – Nesta técnica, o entendimento global sobre uma área específica está contido em um conjunto de regras e o conhecimento específico, importante para uma determinada circunstância, é formado de fatos apresentados por proposições positivas ou negativas que são armazenadas em um banco de dados. Nesse sistema são dois os modos de operação: o direto e o reverso. No primeiro modo, para se chegar à solução do problema deve-se construir uma sequência de passos a partir de um estado inicial. As regras devem ser aplicadas sobre um banco de dados que contenha todos os alarmes recebidos, no caso de ser um sistema de diagnóstico de falhas, até se alcançar uma situação de conclusão que contenha uma falha. No modo seguinte, uma sequência de procedimentos que conduz até a configuração equivalente ao estado inicial é criada a partir da configuração equivalente à solução do problema. As regras devem ser empregadas em um banco de dados que contenha todas as falhas

possíveis, para o caso de um sistema de diagnóstico de falhas, até se obter uma situação de conclusão na qual todos os alarmes recebidos estejam presentes (MEIRA, 1997).

2. Localização explícita – No modelo recomendado pelo ITU-T em (ITU-T X773, 1992). diz que cada notificação de alarme pode conter, entre outras informações, um parâmetro denominado notificações correlacionadas. Quando presente, este parâmetro contém um conjunto de identificadores de notificações e, se necessário, os respectivos nomes associados das instâncias de objetos gerenciados. Em (BOULOUTAS *et al.*, 1994) o modelo utilizado é semelhante ao do sugerido pelo ITU-T, pois a cada alarme é associado um dado sobre localização de falha, baseando-se em um conjunto que contém todas as localizações possíveis. Admite-se que os alarmes são verdadeiros e que exista somente uma falha na rede. Com isso, a falha estará na sobreposição dos conjuntos de localizações apontados pelos diferentes alarmes. Posteriormente, para abranger situações de múltiplas falhas deve-se expandir o cenário, pois na prática não só podem existir falhas simultâneas como também alarmes falsos e perdidos (MEIRA, 1997).

3. Correlação distribuída – A gerência distribuída é utilizada para tratar de um modelo de rede de telecomunicações gerenciada em (KATZELA e SCHWARTZ, 1995). Nesse modelo é denominado de domínio de alarmes todo e qualquer conjunto de objetos gerenciados que enviam alarmes quando da ocorrência de uma falha. O centro de gerência tem que prover o domínio de cada um dos alarmes recebidos antes de começar a atividade de localização de falhas – localização explícita (BOULOUTAS *et al.,* 1994). Cada conjunto de alarmes, cujos domínios têm uma interseção diferente de 0 (zero)– conjunto vazio, pode ter uma ou mais causas possíveis. Dentre essas causas possíveis a mais verossímil deve ser descoberta pelo algoritmo de localização de falhas.

2.3.3.3 Diagnóstico de falhas

Um modelo da configuração gerenciada que processa o fluxo de alarmes em tempo real e seja robusto suficiente para trabalhar com dados truncados é o que se deseja de um bom sistema de diagnóstico de falhas. Dentre outras características importantes de um bom sistema de diagnóstico de falhas, é desejável que ele possa de alguma maneira interpretar os resultados dos testes que foram aplicados para identificar mudanças na aparência e na prioridade dos problemas em função da sazonalidade, separar causa de efeitos e resolver os problemas por ordem de severidade (SUTTER e ZELDIN, 1988)

Para que o problema de correlação de alarmes seja solucionado alguns obstáculos precisam ser vencidos, tais como: centralização do recebimento e armazenamento de alarmes, e conhecimento de como uma falha em um elemento de rede pode afetar os demais elementos adjacentes a ele.

O projeto e o desenvolvimento de algoritmos para fazer a correlação, possuem complexidades intrínsecas a qualquer problema NP-completo, porém, mesmo superadas essas complexidades existem mais alguns parâmetros que precisam ser levados em consideração (HOUCKS *et al.*, 1995):

- Dependências complexas. Normalmente, admite-se que quando um recurso de suporte tem um mau funcionamento, os demais elementos que dependem deste recurso terão também um mau funcionamento, o que nem sempre é verdade;

- Dependências ocultas. A construção de um modelo de rede gerenciada é quase sempre uma das técnicas exigidas para a correlação. Entretanto, alguns elementos de rede podem deixar de ser gerenciados, no processo de correlação, por causa da simplicidade do modelo, com isso falhas ocorridas em elementos não gerenciados podem indicar falha em outro elemento.

- Dados incompletos. Comumente, os elementos de rede enviam para a gerência de rede todos os dados utilizados para a correlação. No entanto, devido à uma interrupção em um enlace sem rota alternativa, estes dados não serão enviados;

- Ruídos. Estes são oriundos de dados redundantes e/ou sem relevância, de alarmes repetidos e/ou transitórios, assim como de alarmes intermitentes.

2.4 REDES ÓPTICAS

2.4.1 Camadas SDH/WDM/Óptica

A camada óptica é denominada de camada servidora, pois providencia serviços a outras camadas que são denominadas de camadas clientes. Dentre essas camadas clientes está a SDH.

Uma conexão entre dois nós de rede, onde um comprimento de onda é dedicado a mesma, em cada ligação do seu trajeto, denomina-se trilha. As camadas clientes empregam as trilhas fornecidas pela camada óptica. Numa rede SDH que opera sobre a camada óptica, as trilhas são simplesmente utilizados para conexões físicas da fibra entre terminais do SDH.

Antes do advento da camada óptica, a camada SDH era a camada predominante na rede de telecomunicações e é ainda a camada dominante em muitas partes da rede. Na camada SDH os circuitos de baixa velocidade são multiplexados e a velocidade destes é elevada para taxas mais altas. Diversos comprimentos de onda e caminhos são combinados juntos por faixas de comprimentos de onda. As faixas são novamente combinadas para formar o sinal WDM dentro da fibra.

Uma única falha poderá ser responsável por gerar uma avalanche de alarmes, por causa da grande quantidade de componentes de rede e do grande tráfego de dados. Isso poderá ocorrer quando um mesmo componente for compartilhado por vários canais. A gerência de re-provisionamento de circuitos será tão eficiente quanto for o processo de localização da falha. A Figura 8 apresenta a multiplexação hierárquica em camadas, onde aparece em destaque a camada óptica.

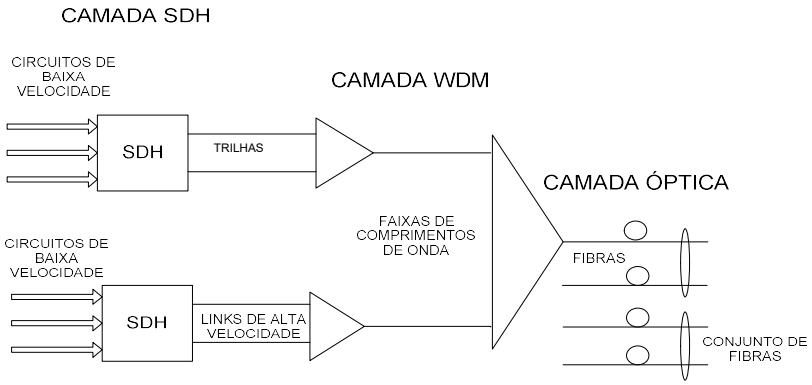


Figura 8. Multiplexação Hierárquica em Camadas. Ramaswami e Sivarajan (2000).

As trilhas que são utilizadas pelos elementos de rede das camadas SDH e Protocolo Internet, IP (*Internet Protocol*) são providenciadas pela camada óptica. Os pacotes de baixa velocidade de circuitos chaveados são multiplexados pela camada SDH para dentro de pacotes de alta velocidade, que são transportados pelas trilhas. O sinal WDM na fibra é composto pela combinação de vários comprimentos de onda.

Em uma rede óptica, se um nó estabelece uma comunicação com outro nó, tem-se um canal. Esse canal utiliza-se de uma rota como meio de acesso para estabelecer a comunicação fim a fim entre os nós. A rota por sua vez, faz parte de uma trilha que pode comportar diversas rotas. A trilha em questão pode ser parte de uma topologia *Lightpath*, topologia de uma rede de comunicação óptica vista pelas camadas de alta ordem (RAMASWAMI e SIVARAJAN, 2000). A seguir definimos os termos importantes do nosso modelo:

1. Elemento/Componente de Rede - será considerado elemento ou componente de rede a fibra e qualquer componente integrante do nó. Entre os componentes de rede há dois tipos de relação, uma que fornece os canais estabelecidos e a outra que apresenta a topologia de rede (MAS *et al.*, 2000). A primeira é denominada de associação e a segunda de interconexão. O estabelecimento da comunicação entre dois nós, onde existe a troca de informação, será considerado neste trabalho como um canal.

2. Associação – A relação entre um nó de rede e um canal é interpretada como uma associação. Caso um componente de rede pertença a um canal, pode-se afirmar que o componente de rede está associado a este canal (MAS *et al.*, 2000). Na Figura 9 existem dois canais, onde o canal 1 é uma sequência ordenada de 5 nós de rede e o canal 2, por sua vez, possui uma sequência ordenada de 4 nós de rede. O nó de rede B, por exemplo, está associado ao canal 1 e é o segundo componente da sequência do canal 1, o nó de rede F é o quarto e o H é o quinto e último componente do canal 1. O mesmo raciocínio é aplicado para o canal 2. Por exemplo, o nó de rede C está associado ao canal 2 e é o segundo nó da sequência do canal 2.

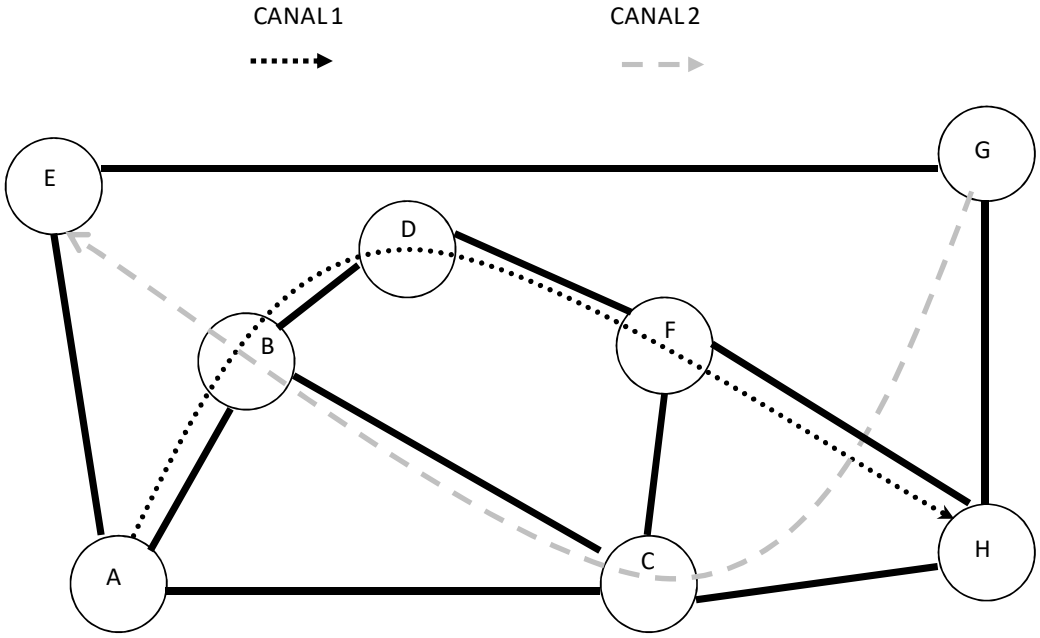


Figura 9. Topologia de uma rede óptica com oito nós e dois canais. Elaborado pelo autor.

3. Interconexão – Se dois nós de rede, aqui representados por círculos, estão conectados fisicamente dentro da rede, então pode-se afirmar que, na Figura 9, o nó de rede B está interconectado com o nó D. Na Figura 9, pode-se ainda observar que o nó E está interconectado com A e G, e não está interconectado com H.

4. Alarmes - As falhas ocorrem quando algum componente de rede não estiver funcionando adequadamente, como, por exemplo, sinal óptico com baixa potência ou algum componente de rede operando fora da faixa de trabalho. Essas falhas, por sua vez, provocam os alarmes que são emitidos para gerência pelos próprios componentes falhos e/ou por outros componentes que pertençam ao mesmo canal. Na próxima seção serão apresentados os componentes que possuem a capacidade de enviar alarmes. No alarme enviado para a gerência existirá a identificação do componente de rede que está enviando o alarme e a condição anormal, que são as informações suficientes para o trabalho proposto.

5. Canal - Um importante fator para ser considerado no projeto de uma rede WDM é a quantidade de comprimentos de onda que serão usados. Em alguns casos, pode ser desejável projetar a rede com o número máximo de canais possíveis. Numa outra situação pode-se desejar atribuir um comprimento de onda diferente para cada nó. Nas grandes redes chamadas, WANs (*Wide Area Network*), o objetivo é normalmente

minimizar o número dos comprimentos de onda para uma determinada topologia da rede ou um teste padrão de tráfego. Em todo o caso, o número máximo dos comprimentos de onda é limitado pela tecnologia do dispositivo óptico utilizado (BORELLA, 1997). O número dos canais é afetado tanto pela banda útil disponível quanto pela faixa espectral dos componentes e/ou afastamento dos canais. Os canais podem ser unidirecionais ou bidirecionais. Todos os canais tratados nesse trabalho são unidirecionais. Sequências ordenadas de componentes de rede são denominadas de canais unidirecionais. Segundo a recomendação M.3100 - TMN, os canais unidirecionais são equivalentes às trilhas, quando o ponto de terminação de origem do caminho for o meio de acesso do transmissor e o ponto de terminação do fim do caminho for o meio de acesso do receptor.

2.4.2 Componentes de rede

Nesta subseção são apresentados os componentes de uma rede óptica, tais como a fibra óptica e dispositivos como: transmissores, receptores, filtro de inserção e derivação, dentre outros. São mostradas as propriedades destes componentes, assim como a classificação dos mesmos em relação ao comportamento na ocorrência de uma falha.

2.4.2.1 Componentes de uma rede óptica

Fibra Óptica: possui muitas características que a torna um meio físico excelente para redes de alta velocidade. Na Figura 10 são mostradas as regiões de atenuação da fibra óptica. Centrada em aproximadamente 1300nm existe uma faixa 200nm em que a atenuação é menor do que 0,5dB/km. A largura de banda nessa região é aproximadamente 25 THz. Centrada em aproximadamente 1550nm existe uma região quase do mesmo tamanho, cuja atenuação é inferior a 0,2dB por quilômetro. Combinadas, essas duas regiões fornecem um limite superior teórico de 50 THz de largura de banda útil. Como pode ser observado na Figura 10, a principal causa da perda em fibras é a dispersão de Rayleigh, que ocorre devido à irregularidades em

nível microscópico na densidade do material, provocando variações no índice de refração, o pico da perda ocorre na região de 1400nm, devido às impurezas na fibra (íon hidroxila – OH^-). Outras fontes da perda incluem a absorção do material e a perda radioativa (Absorção na região dos infravermelhos e ultravioletas).

Se for feito o uso destas áreas de baixa atenuação para a transmissão de dados, a perda do sinal de um ou mais comprimentos de onda pode ser reduzido significativamente, reduzindo dessa forma o número de amplificadores e repetidores. A transmissão na fibra é imune à interferência eletromagnética e também não causa interferência. Finalmente, a fibra é feita de uma das substâncias mais baratas e disponíveis na Terra, a sílica. Isto faz da fibra, um material ecologicamente correto e, ao contrário do cobre, seu uso não esgotará recursos naturais.

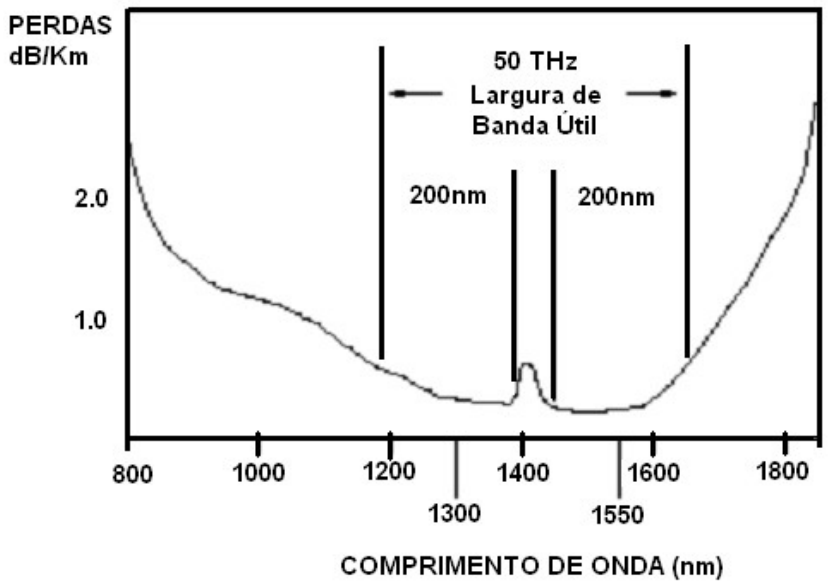


Figura 10. As regiões de baixa atenuação de uma fibra óptica. Borella *et al.*, (1997).

Devido a essas e outras características pode-se afirmar que a fibra possui baixa atenuação, grande capacidade de transmissão, baixo custo e que ela é capaz de transmitir vários canais simultaneamente, onde cada canal utiliza um comprimento de onda.

Transmissor (TX):A palavra-chave é emissão estimulada, que é o que permite que um laser produza feixes de luz de grande coerência (BORELLA *et al.,* 1997). A Figura 12 apresenta um modelo genérico de um laser. Os transmissores usados em redes WDM frequentemente requerem a capacidade de trabalhar com diferentes comprimentos de onda. A largura de banda do laser é a largura espectral da luz gerada pelo laser.

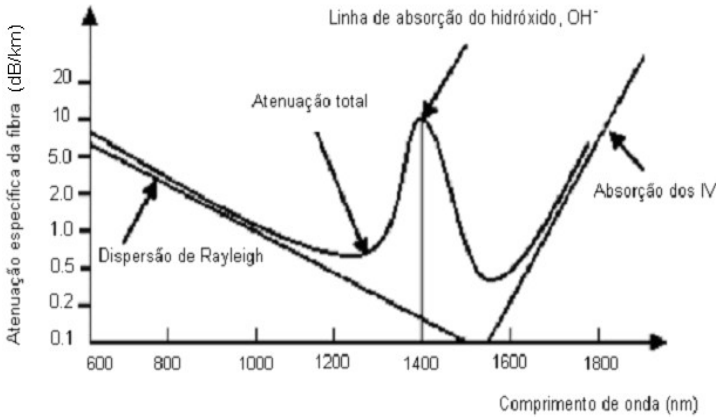


Figura 11. Origem das atenuações nas fibras. Borella *et al* (1997).

O modo de salto ocorre em lasers de injeção-de-corrente, quando uma mudança abrupta na frequência do laser é causada por uma mudança na corrente que alimenta o laser. Os modos de transferência são mudanças na frequência devido às mudanças de temperatura. O gorjeio da frequência é uma variação na frequência devido à variação na corrente de injeção.

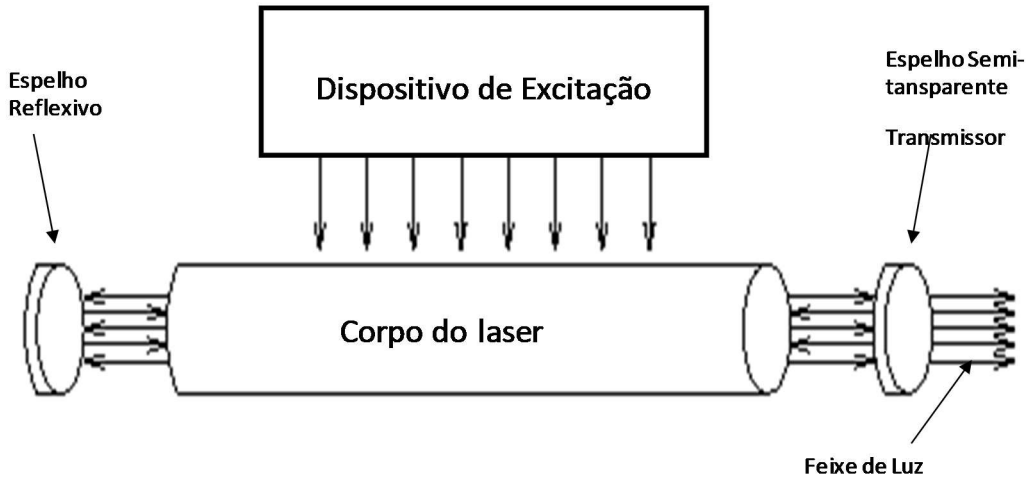


Figura 12. Estrutura geral de um laser. Boloutas *et al.*, (1994).

Em sistemas WDM, as instabilidades da frequência podem limitar o espaçamento dos canais. Os lasers usados nas redes WDM são ajustáveis e podem mudar o comprimento de onda de emissão dentro de uma faixa pré-definida.

Uma matriz de lasers consiste em lasers que são integrados em um único componente e cada um operando em um comprimento diferente. A vantagem de usar uma matriz de lasers é que, se cada um dos comprimentos de onda for modulado independentemente, então múltiplas transmissões podem ocorrer simultaneamente.

O transmissor possui três faixas de trabalho, como pode ser observado na Figura 13.

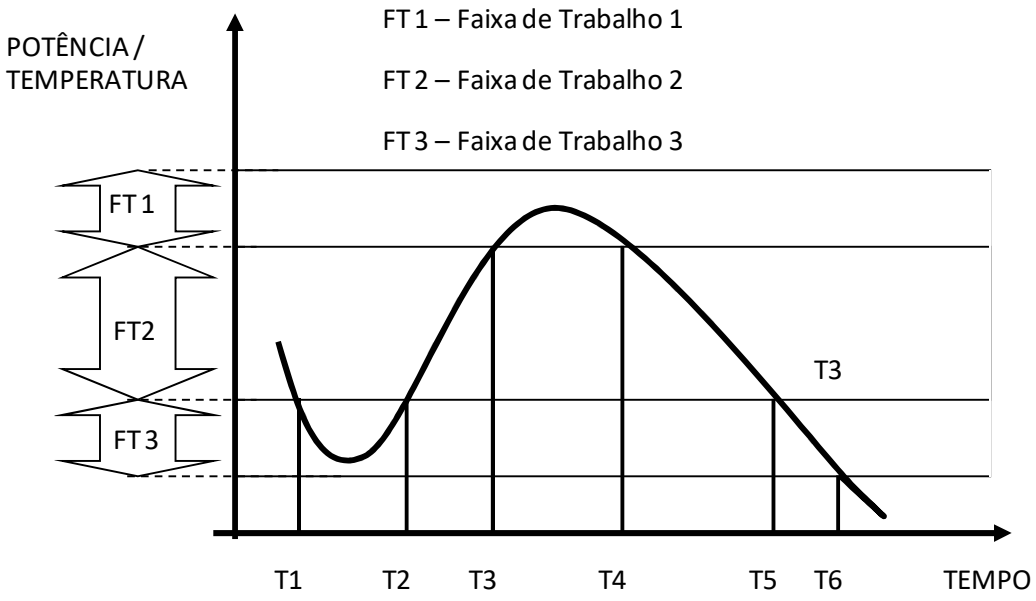


Figura 13. Faixas de Trabalho do Transmissor. Sousa *et al.,* (2005).

Quando a curva da temperatura interna/potência consumida versus tempo transpõe as faixas de trabalho, o transmissor envia um alarme para a gerência. Quando o transmissor estiver operando na faixa de trabalho 2 (T2-T3; T4-T5) ele estará funcionando em condições normais de potência e temperatura, porém, quando o mesmo opera nas faixas de trabalho 1 e 3 (T1-T2; T3-T4; T5-T6) a temperatura e/ou a potência estarão fora dos padrões de operação. Toda vez que a curva de funcionamento do transmissor passa de uma faixa de trabalho para a outra, o transmissor emite um alarme para a gerência, contudo se a curva sair da área das faixas de trabalho, além de ser enviado um alarme para a gerência, o transmissor será desligado para que não ocorram maiores prejuízos. Caso ocorra uma interrupção no envio de dados para o transmissor, devido a uma falha, os componentes de rede que estão após a ele no canal não perceberão o ocorrido, pois o transmissor continuará em comunicação com eles, e eles entenderão, erroneamente, como uma pausa no envio de dados. Desta forma, estará configurado o mascaramento da falha pelo transmissor.

Receptor (RX): A tecnologia de receptores ópticos sintonizáveis é a chave que torna realizável a rede WDM. Nos receptores que empregam detecção direta, um fotodiodo converte potência óptica em corrente elétrica, ou seja, ocorre uma conversão de um sinal óptico em um sinal elétrico. Os receptores ópticos sintonizáveis são caracterizados primeiramente por seus

ajustes de tempo e faixa de operação. A faixa de operação especifica os comprimentos de onda que podem ser acessados pelo receptor. Uma grande faixa de operação permite que os sistemas utilizem um maior número de canais. O ajuste de tempo de um receptor especifica o tempo requerido para mudar de um comprimento de onda para outro. Os receptores enviarão alarmes para a gerência quando a potência do sinal de entrada no mesmo estiver abaixo do valor da potência especificada como referência.

As estruturas tanto de transmissão quanto de recepção estão representadas na Figura 14. Nesta, podemos observar que na transmissão os sinais coloridos (diferentes comprimentos de onda), são multiplexados e saem num único sinal composto por vários comprimentos de onda (sinal branco). Na recepção ocorre o processo inverso.

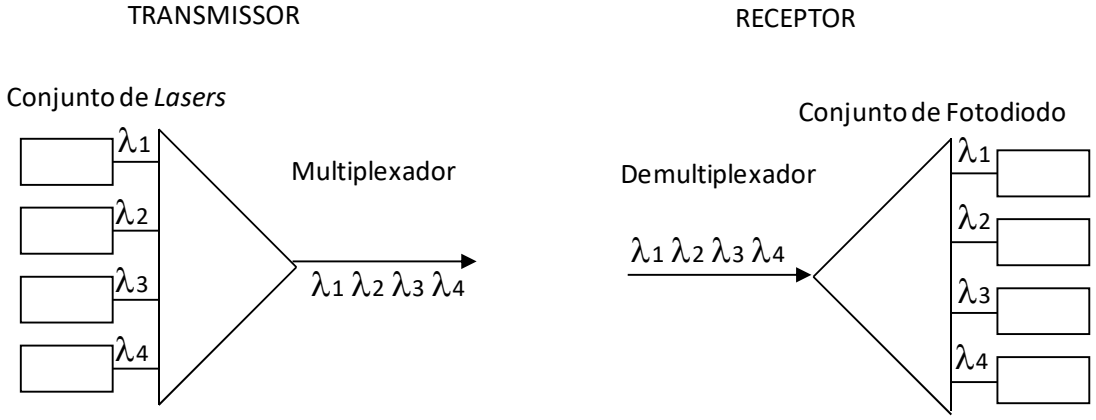


Figura 14. Estrutura de Transmissão e Recepção. Borella (1997).

Filtro de Inserção e Derivação- (Add/Drop Filter - ADF): são componentes de rede que possuem a capacidade tanto de inserir quanto de extrair um determinado comprimento de onda de um sinal óptico que é composto por diversos comprimentos de onda. Nos processos de inserção e derivação não há interferência nos demais comprimentos de onda que compõem o sinal óptico. A principal característica do ADF é a banda passante, que pode degradar com o tempo ou com as condições do meio (variações de temperatura). Esta degradação provoca no ADF variação na frequência central e na sua largura de banda (de 3dB a 20dB) da banda passante, implicando na sobreposição de canais adjacentes. Na ocorrência de um mau funcionamento do ADF o sinal derivado ficará abaixo do valor permitido. Nesta situação, o ADF envia alarme para a gerência e provoca alarmes de outros componentes de rede (receptor

e regenerador) que ficam após a ele no canal. O diagrama funcional do ADF é mostrado na Figura 15.

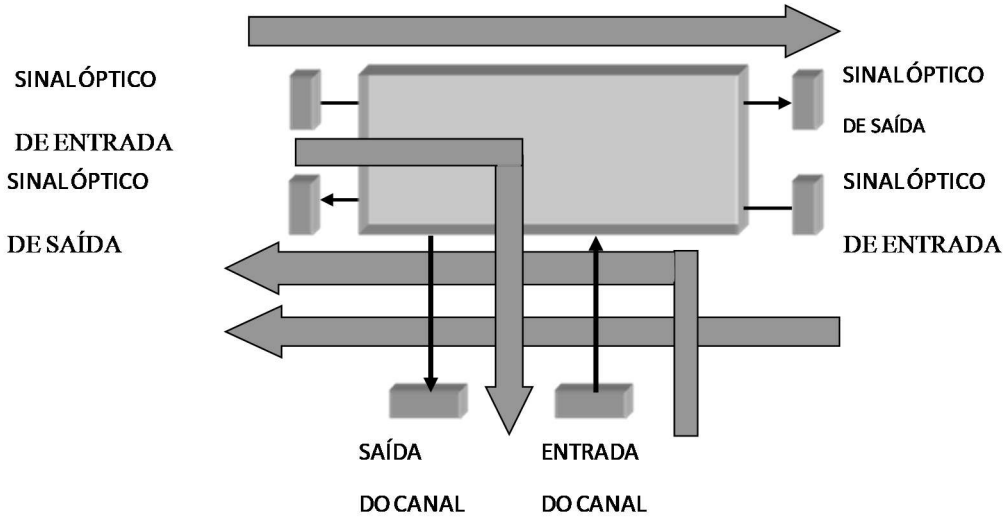


Figura 15. Diagrama do filtro de inserção e derivação. Elaborada pelo autor.

Regeneração, Reformatação e Resincronização (3R): A regeneração consiste na amplificação, sem ruído, do sinal óptico. A reformatação de um sinal reproduz a forma original do pulso de cada bit, eliminando significativamente o ruído. A reformatação é normalmente utilizada em sinais que são modulados digitalmente, mas em alguns casos pode também ser aplicado em sinais analógicos. A resincronização faz o reajuste dos intervalos de tempo entre os pulsos, de acordo com o sinal de origem. A resincronização só é utilizada em sinais modulados digitalmente. Haverá envio de alarme para a gerência quando não for possível fazer o sincronismo do sinal de entrada, devido a este estar com baixa potência.

Comutador de Proteção - (*Protection Switch - PS*): em toda a rede é importante manter a relação sinal ruído em um valor aceitável, a fim de assegurar a detecção do sinal por parte da recepção. Normalmente, em uma rede WDM a potência do sinal pode diminuir devido a duas causas: a atenuação na fibra e perdas de acoplamento. Para resguardar a integridade da recepção o comutador de proteção recebe o mesmo canal (comprimento de onda) replicado dos demoduladores ou dos regeneradores, e opera com aquele que possua o nível de potência aceitável. As escolhas dos comprimentos de ondas de referência são feitas durante as configurações dos canais. Caso o sinal do comprimento de onda de referência não esteja dentro da faixa de potência tolerável, o comutador de proteção irá escalonar uma entrada que possua potência aceitável. No ato do chaveamento para outra entrada ocorrerá um envio de um alarme para a gerência. A estrutura funcional do PS é apresentada na Figura 16.

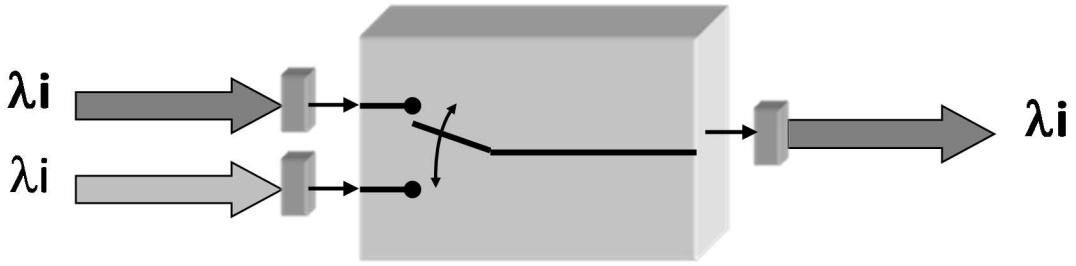


Figura 16. Diagrama do Comutador de Proteção. Elaborada pelo autor.

Comutador - (Switch - SW): comutadores que atuam como dispositivos relacionais estabelecem relações entre entradas e saídas. A relação é uma função de sinais de controle aplicados em um dispositivo e é independente do conteúdo do sinal ou dos dados de entrada (BORELLA, 1997).

Uma propriedade desse comutador é que a informação entra e flui através do mesmo sem sofrer mudanças ou influências da relação corrente entre as entradas e saídas. Essa característica é também conhecida como transparência de dados. Comutadores que atuam como dispositivos lógicos tem o seu estado controlado pelos dados e/ou informações que são transportadas pelos sinais que incidem no mesmo. Iremos considerar os comutadores relacionais e os mesmos serão elétricos, pois a rede será do tipo multi-saltos. Quando ocorre uma falha no comutador que o impossibilita de funcionar adequadamente, ele enviará um alarme para a gerência.

Na Figura 17, um canal, em um comprimento de onda 1 (λ1), pode ser chaveado para a saída do nó, onde ele será convertido para um sinal elétrico ou pode ser retransmitido para outro nó, em um novo comprimento de onda (λ2) ou no mesmo comprimento de onda (λ1).

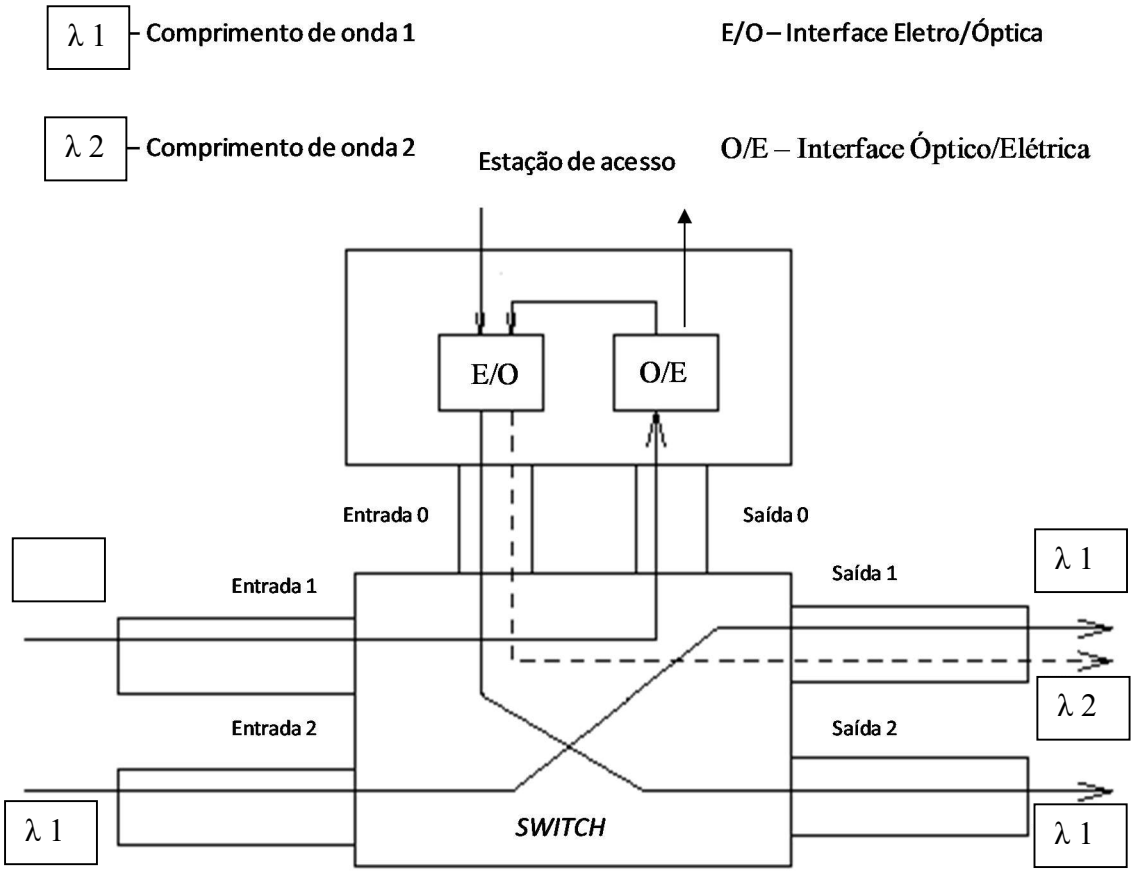


Figura 17. Arquitetura que suporta conversão do comprimento de onda. Borella (1997).

Multiplexador/Demultiplexador (Mux/Demux):O sinal WDM é composto de vários sinais ópticos que são combinados e acoplados pelo multiplexador. O processo no sentido inverso é feito pelo demultiplexador, isto é, a conversão do sinal WDM em diversos sinais ópticos de diferentes comprimentos de onda. Os Mux/Demux não enviam nenhum tipo de alarme, independentemente da falha ser intrínseca a eles ou não.

Exemplos de multiplexador e demultiplexador WDM são mostrados na Figura 18.

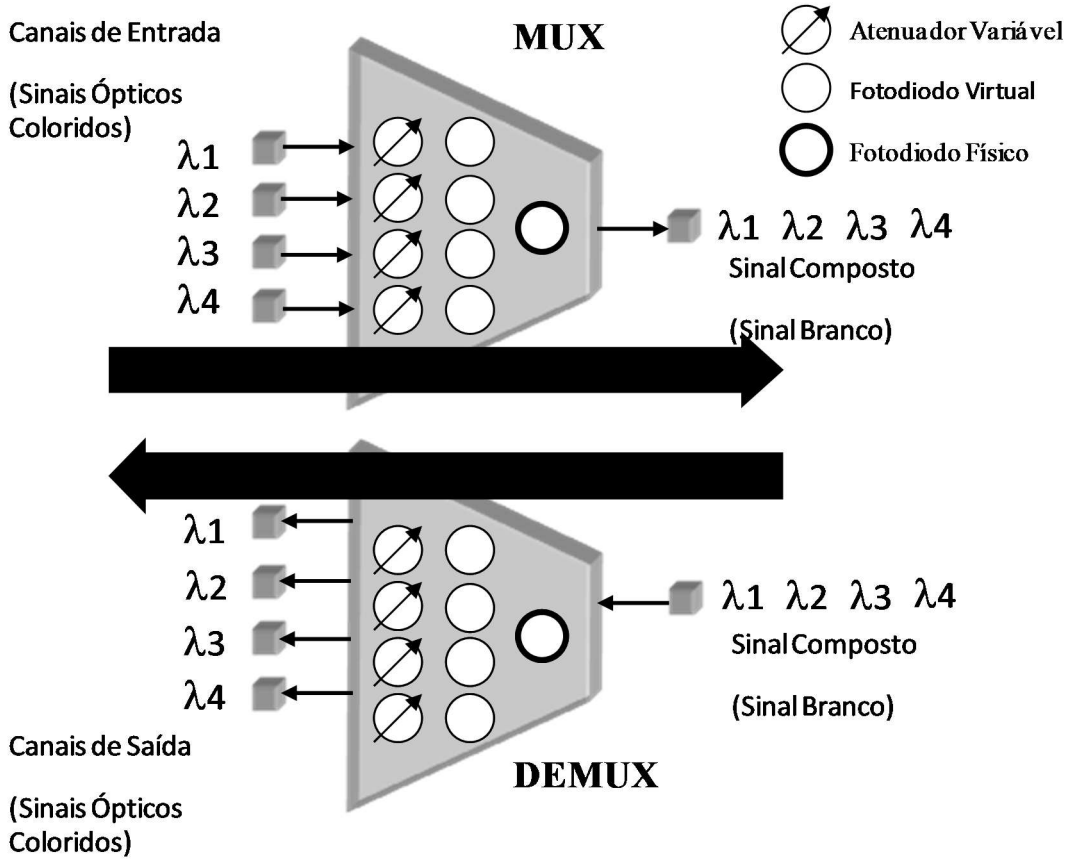


Figura 18. Multiplexador e Demultiplexador. Borella (1997).

Porta de Acesso Local (Local Access Port - LAP) – dispositivo que funciona como interface de acesso do nó a rede. Os nós do nosso modelo inserem ou retiram somente um comprimento de onda. Portanto, o LAP trabalha com um só comprimento de onda e no nível elétrico, visto que, o LAP dentro do canal está após o transmissor e ao comutador, permitindo que o comprimento de onda seja retirado ou adicionado a rede. O LAP não possui a capacidade de enviar alarmes.

2.4.3 PROPRIEDADE DOS COMPONENTES ALARMANTES

No que diz respeito à forma de comportamento dos componentes alarmantes diante de uma falha, podemos dividi-los nos seguintes grupos:

- Alarmantes Internos – são componentes de rede que tem a capacidade de enviar alarme para a gerência quando não estiverem funcionando dentro das especificações

pré-definidas. Os alarmes de equipamentos definidos pela (ITU-T. X.721, 1992) equivalem aos alarmes enviados pelos alarmantes internos. Os protocolos de gerenciamento, tipo SNMP (*Simple Network Management Protocol)* ou CMIP (*Common Management Information Protocol*) são responsáveis pela comunicação entre os Componentes Alarmantes e a gerência.

- Alarmantes Externos – os componentes pertencentes a este grupo enviam alarmes quando ocorre algum evento externo a eles, isto é, eles geram alarmes para o gerente informando uma condição anormal em algum ponto da rede, embora eles não sejam os causadores dos alarmes. Esses alarmes equivalem aos alarmes de comunicação e infraestrutura definidos pela (ITU-T. X.721, 1992). O comutador de proteção se enquadra nesse grupo, pois quando a potência do comprimento de onda da entrada de referência está abaixo do nível aceitável, devido a algum problema anterior a eles, ocorrerá um chaveamento para uma entrada cuja potência esteja em um nível aceitável e o envio de um alarme para a gerência.
- Mascaradores - constituem este grupo os componentes que mascaram os alarmes enviados por componentes anteriores a eles dentro do canal. O que indica se um componente A fica atrás ou na frente de um componente B em um canal é a ordem de passagem do comprimento de onda, ou seja, A estará antes de B caso o comprimento de onda seja detectado primeiro por A depois por B. Devido a essa propriedade, os componentes alarmantes externos que ficarem após aos mascaradores não perceberão as falhas que ocorrerem antes destes e, consequentemente, não enviarão alarmes para a gerência. O único componente de rede que possui a propriedade de mascaramento é o transmissor, pois na ocorrência de um evento antes dele não ocorrerá a interrupção do laser, com isso todos os componentes que fazem parte da recepção do nó seguinte, componentes alarmantes externos, não perceberão a falha, os mesmos entenderão apenas como uma interrupção na transmissão de dados.
-

Na Tabela 2 está o resultado da análise do comportamento dos componentes alarmantes.

Tabela 2 - Classificação dos componentes alarmantes de acordo com o comportamento diante de uma falha (MAS *et al.*, 2000).

Alarmante Interno (A1)	Alarmante Externo (A2)	Mascarador (A3)	COMPONENTE DE REDE
x			FILTRO DE INSERÇÃO E DERIVAÇÃO
x			COMUTADOR
	x		COMUTADOR DE PROTEÇÃO
	x		RECEPTOR
	x		AMPLIFICADOR 3R
x		x	TRANSMISSOR

2.4.4 Classificação dos componentes de uma rede óptica

Os componentes que podem enviar alarmes para a gerência, quando na ocorrência de alguma condição anormal de funcionamento, possuem microprocessador e são denominados de componentes alarmantes. Por sua vez, os componentes que não têm essa capacidade são denominados de componentes passivos (P). Os componentes alarmantes podem ser subdivididos em três subclasses (SOUSA *et al.*, 2005):

a) Alarmantes A1 – enviam alarmes quando não estão funcionando adequadamente.
b) Alarmantes A2 – enviam alarmes informando que outros componentes não estão funcionando corretamente.
c) Alarmantes A3 – estes se comportam como os Alarmantes A1, além de impedir a propagação de alarmes advindos de elementos anteriores a eles.

Na Tabela 3, encontra-se o resultado da classificação dos componentes de rede, segundo a capacidade de enviar ou não alarmes (componentes Passivos - P).

Tabela 3 - Classificação dos componentes de rede de acordo com as propriedades de envio de alarmes (MAS *et al.*, 2000).

CATEGORIA	*SÍMBOLO*	*COMPONENTE DE REDE*
P		PORTA DE ACESSO LOCAL
P		MULTIPLEXADOR
P		DEMULTIPLEXADOR
P		FIBRA
A1		**FILTRO DE INSERÇÃO E DERIVAÇÃO**
A1		COMUTADOR
A2		COMUTADOR DE PROTEÇÃO
A2		RECEPTOR
A2		AMPLIFICADOR 3R
A3		TRANSMISSOR

2.4.5 Sentenças e análises funcionais da rede e de seus componentes

Devido às características de cada componente de rede, tais como faixa de trabalho, comportamento diante de um evento ou até mesmo o tipo de configuração, podemos observar que algumas premissas devem ser seguidas para termos o correto funcionamento da rede e uma maior eficiência durante o processo de localização de falhas.

2.4.6 Composições dos nós

No modelo de rede utilizado, cada nó utiliza um comprimento de onda diferente e cada conexão entre dois nós possui duas fibras, uma para cada sentido de comunicação. Dessa forma, um dado endereçado a um nó pode alcançá-lo por pelo menos dois caminhos diferentes, o comutador de proteção decidirá qual das duas ou mais entradas será utilizada de acordo com o sinal de melhor nível de potência. Um nó pode ser classificado como nó central ou nó local. Um nó central possui a capacidade de realizar a comutação entre os diferentes comprimentos de onda, o que é possível devido à presença do comutador no mesmo. Esta capacidade também permite ao nó central conectar-se a vários nós da rede. Por sua vez, o nó local se caracteriza pela presença do filtro de inserção e derivação. Os componentes se repetem pela rede formando

os nós, assim, quando uma falha ocorre em algum destes, é necessário saber exatamente qual dos componentes está apresentando a falha e a qual nó ele pertence. Para tornar essa descoberta possível, cada componente deve possuir uma identidade única na rede. No modelo de rede utilizado neste trabalho, esta identificação é formada por quatro campos (A, B, C, D), e eles podem receber um número natural e possuem os seguintes significados para um dado nó local (SOUSA *et al.*, 2005):

- A: indica a categoria do componente quanto ao envio de alarme para a gerência, podendo assumir os seguintes valores:

  0 – Passivo;

  1 – Alarmante interno;

  2 – Alarmante externo;

  3 – Alarmante mascarador.

- B: indica o número do nó na rede.

- C: para o nó local será sempre 0.

- D: identifica o componente dentro do nó. Os valores para este campo variam de acordo com os componentes e são os seguintes:

  LAP = 0;

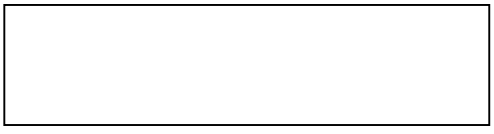
  ADF = 1 SH ou 2 SAH;

  RX = 1 SH ou 2 SAH;

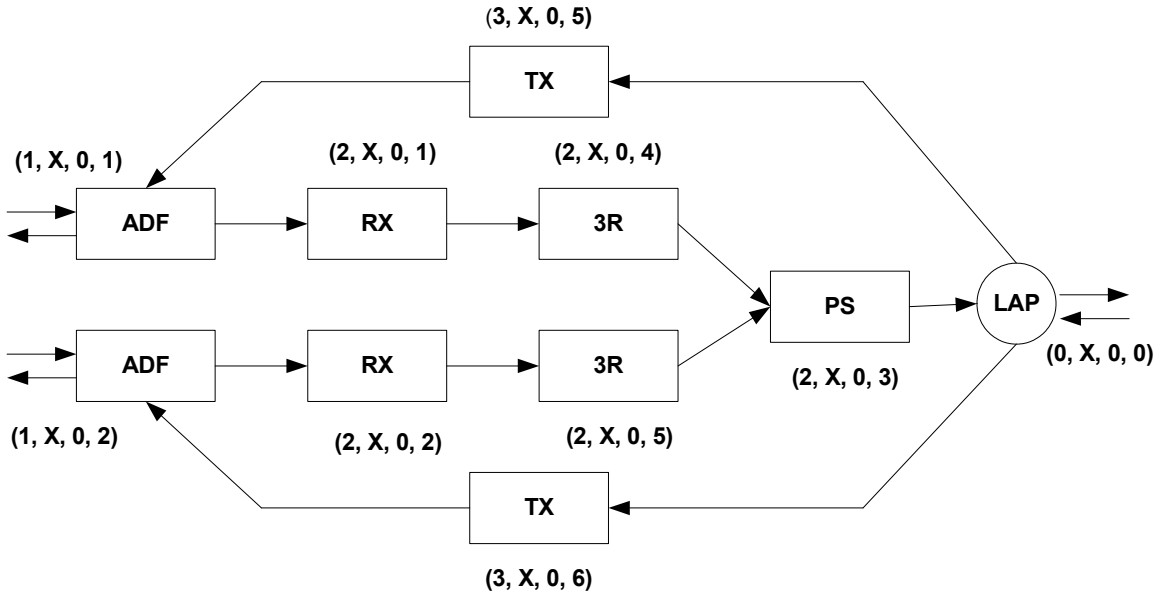
  3R = 4 SH ou 5 SAH;

  TX = 5 SH, 6 SAH;

  PS = 3.



A Figura 19 apresenta a identificação dos componentes para o nó local “X”:



Para um nó central, os campos A e B têm o mesmo significado dos campos correspondentes no nó local. Os outros dois campos, C e D, são usados em conjunto para identificar o componente no nó. Diferentemente do nó local, para o nó central esta identificação é diferenciada para cada componente. Para os componentes LAP, comutador e Multiplexador, os valores para estes campos C e D são fixos: LAP: (0,0); comutador (0,1); Mux: (1,0). Para o componente Demultiplexador, o campo C tem valor 0 e o campo D o número do nó anterior dentro do canal, ao nó corrente, ao qual pertence o Demultiplexador. A identificação dos demais componentes utilizará a informação do comprimento de onda tratado por cada um deles. Cada nó tem um comprimento de onda associado, designado por λz, onde Z é o número do nó. Um canal é estabelecido utilizando o comprimento de onda do nó no qual se inicia. No entanto, após o primeiro comutador, o comprimento de onda do canal será comutado para o valor do comprimento de onda do nó, onde o mesmo irá terminar. Assim, o Canal 1 (CH 1) estabelecido entre os nós X e Y da rede, utiliza inicialmente o comprimento de onda λx e após passar pelo primeiro comutador passa a utilizar o comprimento de onda λy.

Na identificação dos componentes: transmissor, comutador de proteção, receptor e amplificador 3R, que tratam os comprimentos de onda individualmente, os campos C e D assumem os seguintes valores: TX-(0, Z); PS-(Z, 1); RX-(Z, 2); 3R-(Z, 3), onde Z é o número do comprimento de onda que está sendo transportado pelo componente. A Figura 20 apresenta a identificação dos componentes para o nó central “X”:

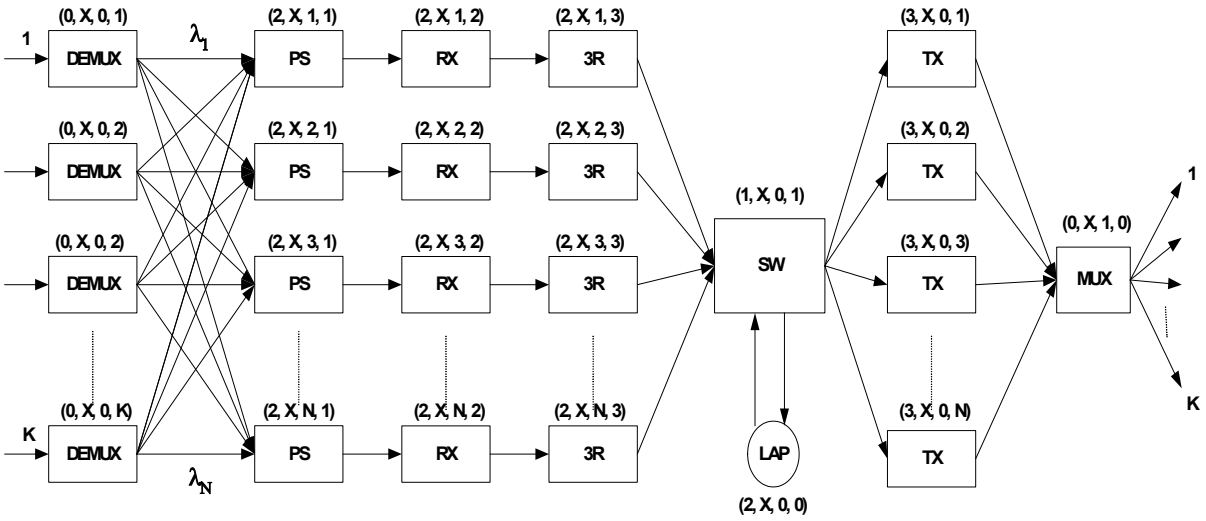
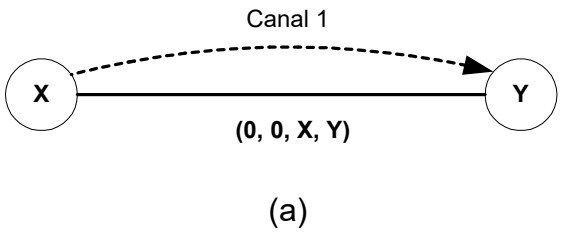


Figura 20. Identificação dos componentes no nó central "X". MAS *et al.*, (2000).

A fibra óptica também recebe uma identificação no mesmo formato dos demais componentes. Esta identificação é feita em cada *link* de interconexão entre os nós. O significado de cada campo e os valores que estes assumem são: A=B=0; C recebe o número do nó anterior para o canal; D recebem o número do nó posterior para o canal; A Figura 21.a mostra a identificação para a fibra que interliga os nós X e Y para o Canal 1, com o sentido de comunicação de X para Y. A Figura 21.b identifica a fibra entre os nós X e Y para o Canal 2, com sentido de comunicação de Y para X.



(a)

Figura 21. Identificação da fibra entre os nós X e Y para os canais 1 e 2. Elaborada pelo autor

2.4.7 Falhas de elementos de rede

As falhas ocorrem quando pelo menos um elemento de rede não estiver funcionando corretamente. Estas falhas podem provocar alarmes que serão emitidos para a gerência pelos próprios componentes falhos ou por outros componentes que pertençam ao mesmo canal.

Seguindo um conjunto de regras que foram formadas de acordo com o comportamento e categoria de cada componente, obtêm-se as normas gerais de comportamento perante falhas:

- Os alarmes emitidos pela quebra ou mau funcionamento do Multiplexador, Demultiplexador e fibra serão iguais, caso estes pertençam ao mesmo canal. Os componentes que enviarão alarmes serão: comutadores de proteção, receptores e amplificadores 3R's. Isso significa que o sinal óptico foi interrompido e, como consequência, todos os canais são interrompidos, isto é, os λs param de ser transmitidos. Vale ressaltar que a quantidade de trios de recepção (comutadores de proteção, receptores e amplificadores 3R's) que enviarão alarmes depende da quantidade de canais que passam pelo componente falho.
- Se a falha no transmissor provocar interrupção do canal, os alarmes serão gerados pelo transmissor e por um dos trios de recepção de um nó posterior ao nó do transmissor, notadamente, o trio em questão trabalha com o mesmo comprimento de onda do transmissor.
- Uma falha no ADF de um nó local, que utilizado como passagem provocará a emissão de alarmes dos seguintes componentes: comutador de proteção, receptores e amplificadores 3R's. A quantidade de trios que enviarão alarmes dependerá do número de canais que passam pelo ADF.

2.4.8 Sentenças e análises operacionais da rede e componentes

Após observações e análises dos comportamentos individuais e em conjunto dos componentes que pertencem à rede chegamos a algumas proposições que são apresentadas nas Subseções 3.4.8.1 a 3.4.8.4.

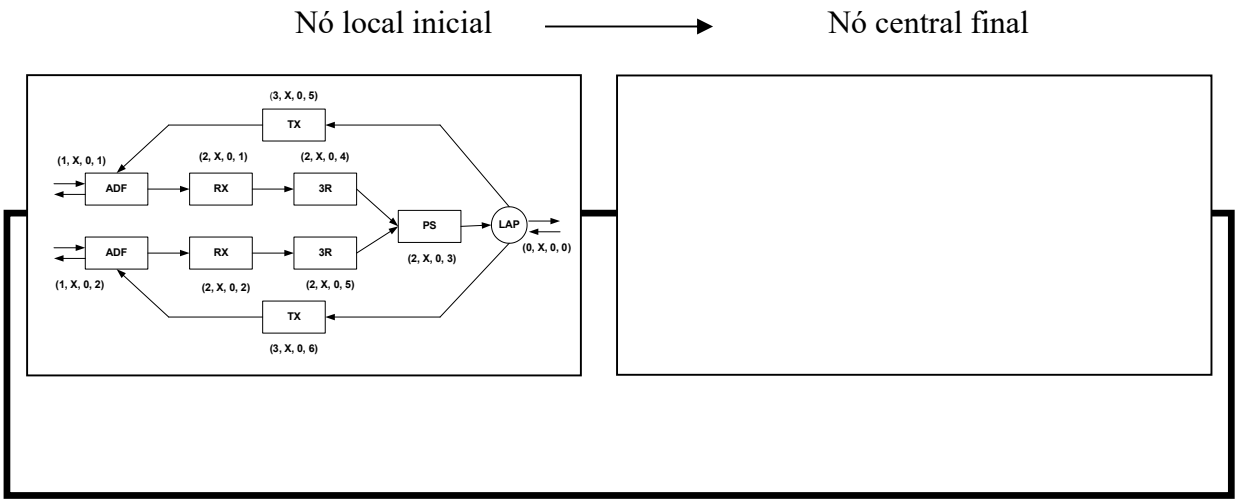
2.4.8.1 *Considerações da topologia*

Para toda e qualquer topologia será necessária a inclusão de um nó central, pois sem a presença do mesmo, o chaveamento dos comprimentos de onda - mudança de um comprimento de onda para outro - não será possível. Para comprovar a proposição descrita, considere o funcionamento do nó local estando configurado como inicial ou final.

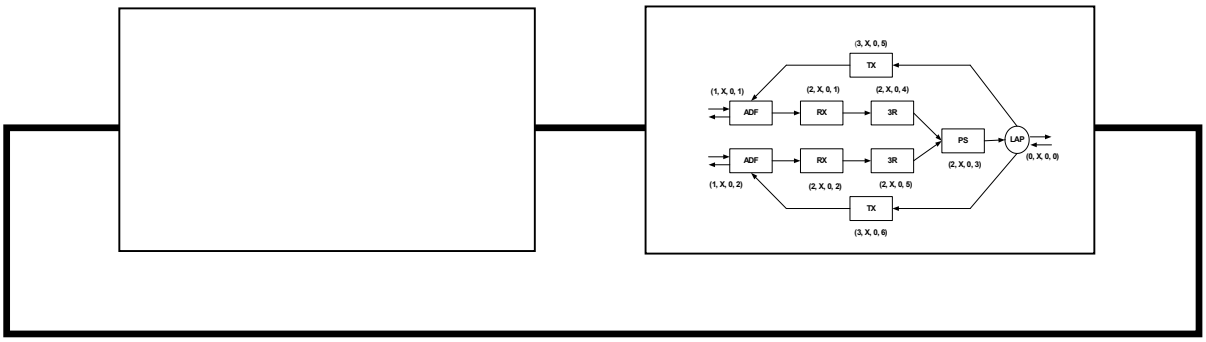
O nó local está limitado a trabalhar internamente apenas com um canal, ou seja, um e somente um comprimento de onda devido à limitação do ADF, que só permite a inclusão e a extração de um único comprimento de onda do sinal óptico. Então, se o nó local trabalha apenas com o comprimento de onda dele próprio, surge a seguinte indagação: "Como o nó local se comunica com os outros nós, sejam eles locais ou centrais?" A resposta é simples: "Através do nó central". A razão é que na estrutura interna do nó central existe um comutador que possibilita a conexão-cruzada, ou seja, permite que se associe um determinado λ (comprimento de onda) de entrada com um determinado λ de saída.

Portanto, devido à forma de funcionamento do nó local, em qualquer topologia o nó central será um elemento de rede obrigatório. Isto implicará em algumas restrições no que diz respeito às configurações de rede, como apresentadas nas Figuras 22 a 25:

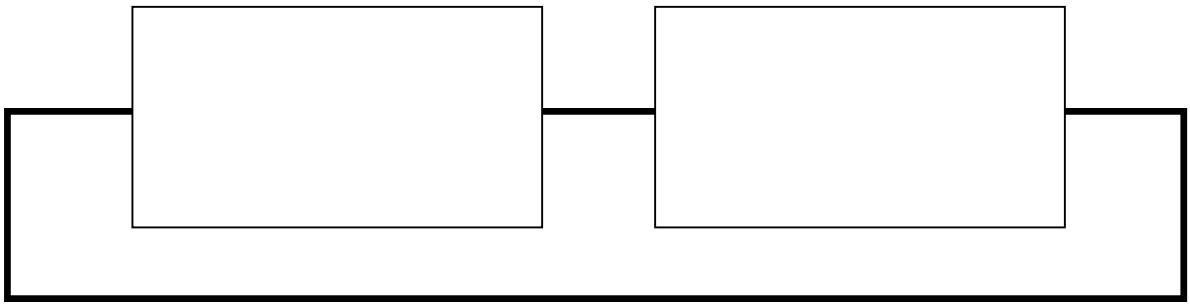
- Menores configurações de rede



Nó central inicial ⟶ Nó local final

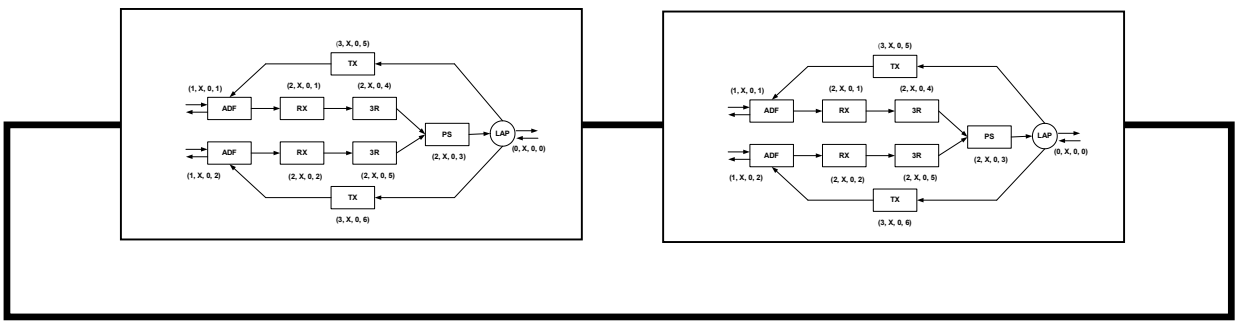


Nó central inicial ⟶ Nó central final



❖ Configuração de rede não permitida (impraticável).

Nó local inicial ⟶ Nó local final



Nota: Não só a configuração acima não será implementável, assim como quaisquer outras que possuam em suas composições apenas nós locais.

2.4.8.2 *Falha do amplificador 3R*

Visto que o amplificador 3R pertence à categoria A2, a ocorrência de uma falha nele em nós centrais não será detectada, pois considerando os dois tipos de configuração do nó central que fazem uso do amplificador 3R, têm-se os seguintes componentes logo após:

- na configuração de passagem do nó central

  Comutador ==> Transmissor ==> Multiplexador

- na configuração final do nó central

  Comutador ==> Porta Local de Acesso

Observando a configuração de passagem, nota-se que uma falha no amplificador 3R não será percebida por nenhum componente do nó ao qual o amplificador 3R pertence e por nenhum componente de um nó adjacente, devido o transmissor mascarar a falha, pois os mesmos são da categoria A1, A3 ou P. O comportamento observado na configuração de passagem é equivalente para a configuração final, pois a ocorrência de falha no amplificador 3R não implicará no envio de alarmes para a gerência, devido os componentes que sucedem o amplificador 3R não pertencerem à categoria A2. Este comportamento de não percepção da falha do 3R não ocorre em nós locais, pois após a ele há um componente de categoria A2 (comutador de proteção).

Caso seja considerada a camada IP pode-se diminuir o problema em questão em 50%, pois admitindo que o nó central esteja na configuração final, a falta do sinal óptico será percebida pelo componente pertencente à camada IP (exemplo: roteador). Esta solução será tema de estudos futuros.

2.4.8.3 *Falha no LAP*

Analisando o comportamento da porta local de acesso podemos notar que a falha neste, tanto em nós centrais, quanto em nós locais, na configuração inicial, não será detectada, devido aos dois nós terem nesse tipo de configuração, os seguintes componentes após a LAP:

- na configuração inicial do nó Local

Porta Local de Acesso ==> Transmissor

- na configuração inicial do nó Central

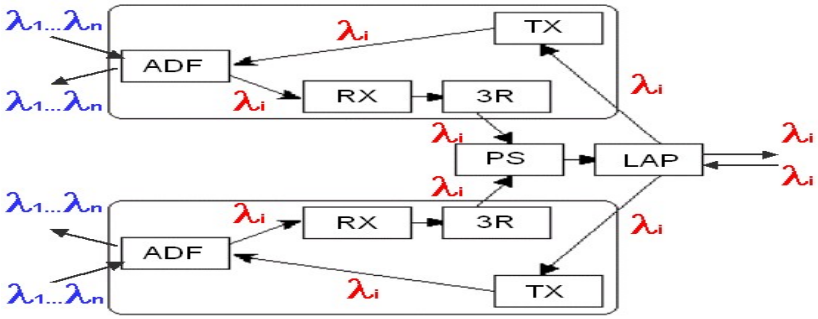
Comutador ==> Transmissor ==> Multiplexador

Lembrando que a LAP não emite nenhum alarme, que para o comutador é transparente a ocorrência de falhas que não sejam inerentes a ele, e que o transmissor mascara falhas para os componentes subsequentes, então, na configuração inicial de ambos os nós (locais e centrais), não haverá emissão de alarmes para a gerência.

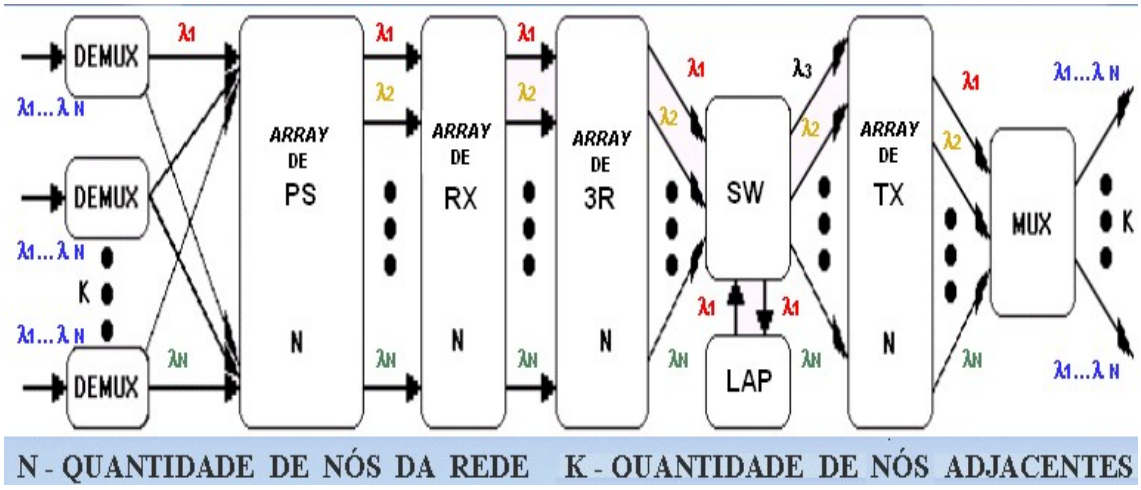
2.4.8.4 *Comportamento dos nós em relação aos comprimentos de onda*

Como os nós locais e centrais possuem componentes diferentes e características de funcionamento também diferentes, a forma que o comprimento de onda é tratado internamente em cada nó também é diferenciada.

Na Figura 26 pode-se observar o comportamento do nó local e o tratamento que ele faz no sinal óptico. Pode-se notar que, internamente ele trabalha apenas com um comprimento de onda, não importando o sentido do canal e nem se o nó é inicial ou final.



Na Figura 27, é apresentado o comportamento do nó central em relação ao sinal óptico. Como podemos notar, internamente ele pode trabalhar com diferentes comprimentos de onda. Isso é possível devido ao comutador que possibilita a mudança de comprimentos de onda.



2.5 RESILIÊNCIA EM REDES DE COMUNICAÇÃO

As redes de telecomunicações atuais estão experimentando um aumento crescente na demanda por capacidade, originada principalmente devido ao sucesso da *Internet*. Para suportar essa demanda, as redes de transporte estão sendo migradas para redes ópticas, por conta das mesmas poderem prover essa demanda. Com o crescimento exponencial das redes de comunicação, os operadores de redes passaram a necessitar de ferramentas poderosas de monitoração e gerenciamento. Para que fosse possível desenvolver essas ferramentas, foi necessária a implantação de uma padronização dos sistemas. Os trabalhos para padronização da *Hierarquia Digital Síncrona – SDH (Synchronous Digital Hierarchy*) tiveram início com o grupo de estudos do *Consultative Committee for International Telegraph and Telephone,* CCITT (atual *International Telecommunication Union Telecommunication Standardization Sector, ITU-T*) em junho de l986. O objetivo desses estudos era criar um padrão mundial para os sistemas de transmissão síncrona que proporcionasse aos operadores de rede um sistema mais flexível e econômico. Foi a padronização desses equipamentos SDH que veio fornecer a

flexibilidade necessária aos operadores de rede para gerenciar eficientemente o crescimento da rede e o provisionamento de novos serviços esperados.

Dentre as várias atribuições de um administrador de redes, os estudos voltados para o aumento da robustez em relação a falhas e ataques são um tema de grande importância. As decisões sobre onde investir de maneira eficiente a um custo justificado são tomadas de acordo com a experiência de cada administrador. Apesar de serem levadas em consideração algumas informações relativas a operação da rede, o processo é muito subjetivo e pode acarretar em decisões equivocadas (VASCONCELOS e SALES, 2012). Conforme os autores, a resiliência em redes de computadores é um tema bastante relevante, sendo alvo de constantes estudos pela comunidade acadêmica. Considerando resiliência como a habilidade de uma entidade de tolerar, resistir e automaticamente se recuperar de desafios nas condições da rede, ataques coordenados e anomalias no tráfego (AGGELOU, 2008), pode-se verificar que a definição é bastante genérica, o que permite o estudo e aplicação da resiliência por meio de diversas técnicas distintas.

Vasconcelos e Sales (2012) afirmam que uma primeira ideia que pode ser vinculada à resiliência de uma rede é a quantidade de redundâncias que a mesma possui. De maneira intuitiva, uma topologia completamente conectada é mais resiliente do que uma rede que não possui redundância. Quando se compara esses dois tipos de topologia, torna-se fácil perceber a diferença em termos de resiliência, entretanto o que existe na prática são situações intermediárias, difíceis de atribuir uma classificação de acordo com a sua resiliência.

2.6 O IMPACTO DA OCORRÊNCIA DE FALHAS EM REDES DE COMPUTADORES

A realização de atividades relacionadas ao processo de gestão de riscos nas empresas pode gerar uma grande quantidade de dados relativos a riscos, que muitas vezes não podem ser devidamente avaliados, revisados e priorizados. Muitas organizações tem utilizado a análise de impacto relativa aos riscos, no sentido de estimar o efeito potencial dos riscos nas operações essenciais ao negócio. Para isso, uma das primeiras necessidades dessas organizações é a identificação dos pontos potenciais de riscos relacionados às suas redes de computadores. Os processos de negócio que dependem dos sistemas (e consequentemente da rede que suporta os mesmos), devem ser classificados de acordo com seu grau de criticidade e tratados em função

dessa classificação. O impacto para o negócio é fundamental para o tratamento dos riscos que envolvem esses processos, entre esses os riscos relacionados à infraestrutura de redes.

O tempo de inatividade em uma rede de computadores pode afetar uma empresa de várias maneiras, gerando principalmente impactos financeiros. Para se estimar o custo que uma falha de rede poderia gerar para uma empresa, torna-se necessário a obtenção de estatísticas que envolvem os atores do processo de utilização dos serviços dependentes da rede, em relação a ocorrência de falhas de rede e informações financeiras atuais. O tempo de inatividade da rede também pode causar uma perda na reputação da empresa e fidelização do cliente. Por exemplo, o fato de um cliente estar aguardando para realizar um pagamento em uma empresa firmada comercialmente, enquanto seus sistemas estão parados, pode causar perda de fidelidade a curto prazo. A mesma situação em uma nova empresa pode fazer com que alguns clientes não retornem. Essa relação de causa e efeito pode ser melhor ilustrada através do exemplo de uma loja virtual que não consegue processar uma transação. O impacto do tempo de inatividade em qualquer rede de computadores não será o mesmo em todos os mercados verticais. Exemplos de mercados verticais incluem, varejo (o tempo de atividade durante os principais períodos de vendas é essencial, como por exemplo, no Natal), o setor público (existem metas governamentais para serem atendidas), serviços profissionais (perda de renda e reputação) e fabricação (a maquinaria computadorizada pode parar a produção ou fazer com que as atualizações do inventário de estoque não estejam disponíveis). As empresas que dependem de sua habilidade para a entrega de serviços de rede e TI para seus clientes, tais como provedores de serviço na nuvem e empresas de comércio eletrônico, são extremamente impactadas por falhas que ocasionam parada em suas redes.

Para poder quantificar o valor monetário, percebido, ou uma possível perda com algum grau de precisão, os gestores de TI precisam pensar sobre o número de funcionários que não poderão trabalhar devido à dependência em relação aos serviços de TI. Manter uma alta disponibilidade dos serviços de TI é um dos fatores essenciais para o negócio. Dessa forma, a disponibilidade é um dos principais objetivos de negócio que norteiam a gestão dos serviços de redes de computadores. Foi identificado que alguns aspectos que influenciam a qualidade do serviço de redes impactam nos resultados do negócio. Por exemplo, o monitoramento e avaliação das métricas de desempenho de disponibilidade em uma rede, como o tempo de reparo de uma falha e o tempo médio entre falhas passaram a ter uma importância estratégica, além da importância já existente ao nível operacional.

Em um nível conceitual mais alto, a disponibilidade de serviços de TI é um dos focos importantes no gerenciamento de serviços. Conforme OP services (2017) são apresentados na sequência os indicadores de desempenho mais ligados ao gerenciamento de disponibilidade do ITIL e suas respectivas formas de estimativa.

1. Disponibilidade (excluindo o tempo de inatividade planejado)

Percentagem do tempo real de funcionamento (em horas) do equipamento em relação ao número total de horas de funcionamento previstas (em horas).
Tempo de funcionamento planejado = horas de serviço – tempo de inatividade planejado
O tempo de inatividade planejado é o tempo de inatividade conforme agendado para manutenção. Também conhecido por: *Service Outage Duration*
Fórmula: [Tempo de atividade real] porcentagem de [Tempo de atividade planejado]
Unidade: Porcentagem
Direção: Maximizar

2. % da interrupção devido a alterações (indisponibilidade planejada)

Percentual de indisponibilidade devido à implementação de mudanças planejadas, em relação às horas de serviço.
Fórmula: [Interrupção devido a mudanças planejadas] porcentagem de [interrupção total]
Unidade: Porcentagem
Direção: Minimizar

3. % da interrupção devido a incidentes (indisponibilidade não planejada)

Porcentagem de interrupção (indisponibilidade) devido a incidentes no ambiente de TI, em relação às horas de serviço.
Unidade: Porcentagem
Direção: Minimizar

4. % de indisponibilidade / indisponibilidade imprevista devido a alterações

Porcentagem de indisponibilidade imprevista (indisponibilidade) devido à implementação de mudanças na infraestrutura. Não planejado significa que a interrupção (ou parte da interrupção) não foi planejada antes da implementação da alteração.
Fórmula: [Queda total não planejada devido a mudanças] porcentagem de [Total de interrupções não planejadas]
Unidade: Porcentagem
Direção: Minimizar

5. % da disponibilidade do Service Desk

Cálculo da disponibilidade da Central de Serviços durante o Período de Relatórios.
Unidade: Porcentagem
Direção: Maximizar

6. % de SLAs de disponibilidade atendidos

Porcentagem de disponibilidade Acordos de Nível de Serviço (SLAs) cumpridos.
Fórmula: [número de SLAs de disponibilidade atingidos] porcentagem de [número de SLAs de disponibilidade]
Unidade: Porcentagem

Direção: Maximizar

7. % de componentes de infraestrutura (críticos) com monitoramento automático de disponibilidade
Percentagem de componentes de infraestrutura (críticos) com monitoramento automatizado de disponibilidade.
Unidade: Porcentagem
Direção: Maximizar

8. % de processos críticos de negócios não cobertos por um plano de disponibilidade de serviço definido
Porcentagem de processos de negócios críticos não cobertos por um plano de disponibilidade de serviço definido.
Unidade: Porcentagem
Direção: Minimizar

9. Falhas de tempo crítico
Número de falhas de serviços de TI durante os chamados tempos críticos. Tempo crítico é o tempo que um serviço deve estar disponível, por exemplo para sistemas financeiros durante o fechamento dos livros (no final do mês ou no final do trimestre).
Unidade: Número
Direção: Minimizar

10. Falha total de tempo crítico
Falha total em falhas de tempo crítico em serviços de TI. Tempo crítico é o tempo que um serviço deve estar disponível, por exemplo para sistemas financeiros durante o fechamento dos livros (no final do mês ou no final do trimestre).
Unidade: Porcentagem
Direção: Minimizar

11. Número de interrupções de negócios causadas por problemas
Número de interrupções de negócios causadas por problemas (operacionais).
Fórmula: SOMA (interrupções de negócios causadas por problemas)
Unidade: Número
Direção: Minimizar

2.6.1 Análises relacionadas às falhas em redes

A realização da análise de impacto sobre o negócio (*Business Impact Analysis - B.I.A.*) relativa à interrupções de serviços de redes pode ser realizada em quatro etapas:

Etapa 1: Definir as principais funções do negócio, identificando as principais funções que estejam associadas ou dependentes do uso de TI. Essas funções podem variar de um processo ou produto para o serviço fornecido por uma empresa, ou seja, instalações de *e-mail*, pesquisa

na *internet* e inventário de estoque. Para uma empresa que opera na *internet*, a capacidade de as transações financeiras ocorrer é uma função comercial básica.

Etapa 2: Priorizar as funções do negócio. Após a identificação das principais funções do negócio, é necessário identificar e priorizar as funções de negócio que são afetadas quando ocorre uma falha que interrompa o serviço de rede. Isso pode ser conseguido ao se determinar o processo e a escala de tempo para a restauração da rede. Algumas funções possuem um custo de interrupção maior que outros, como por exemplo em uma empresa de transporte, o aplicativo de rastreamento de pacotes é a função comercial crítica, devendo ser restaurada imediatamente.

Etapa 3: categorizar o impacto do tempo de inatividade da rede. O impacto do tempo de inatividade da rede pode ser classificado em quatro categorias:

- *Pessoas* - quantos funcionários ficarão inativos quando o serviço de rede é interrompido? (isso pode levar em conta o custo da mão de obra)
- *Propriedade* - Qual equipamento será necessário para substituição?
- *Sistemas* - Quanto tempo demoraria para recuperar os sistemas, para que a empresa continue funcionando normalmente? (a probabilidade de uma falha particular e o tempo necessário para reparar)
- *Dados* - Identificando os dados que são essenciais para garantir a continuidade do negócio - (como os dados essenciais serão recuperados?)

Etapa 4: Classificando tipos de interrupção, frequências e duração. É importante analisar os dispositivos (elementos de rede) nos quais a rede depende, pois alguns dispositivos possuem um alto custo de acordo com o tempo de inatividade. Determinar o tempo de inatividade relacionado às redes também exige um conhecimento sobre as configurações de *hardware* e *software* que fornecem suporte para as principais funções do negócio. Torna-se necessário a identificação dos possíveis pontos de falha em relação às configurações de *hardware* e *software* e, em seguida, quantificar os custos horários associados às interrupções dos sistemas dependentes da rede.

A sigla CAPEX (*CAPital EXpenditure*) significa *Despesas de Capitais* ou *Investimentos em Bens de Capitais*. O CAPEX envolve todos os custos relacionados à aquisição de equipamentos e instalações que visam a melhoria de um produto, serviço ou da empresa em si. CAPEX pode ser considerada a medida básica para se calcular o *Retorno sobre o Investimento*(ROI) em determinado projeto. O termo OPEX (*OPerational EXpenditure*), ao

contrário do CAPEX, possui foco nas *Despesas e Dispêndios Operacionais* e no *Investimento em Manutenção de Equipamentos*, ou seja, são os gastos cotidianos. Uma estratégia empresarial não será completa e boa o suficiente sem considerar um estudo e planejamento nos investimentos com aquisições, manutenções e substituições de ativos fixos. CAPEX e OPEX apresentam impactos diferentes em projetos, pois a maior parte das despesas de capital é fixa e seu impacto financeiro em um projeto é sentido imediatamente. Já as despesas operacionais são incorridas ao longo de toda a vida de um projeto e incluem um componente variável que pode ser gerenciado continuamente. A gestão dos riscos envolvidos possibilita aos gestores um suporte mais efetivo nas análises referentes aos investimentos, como por exemplo, na redundância de pontos críticos de uma rede óptica. Busca-se encontrar uma solução ideal para implementação dos esquemas de sobrevivência com menor impacto no custo da rede.

O processo de quantificação dos custos horários de falhas poderia ser alcançado através da identificação dos tipos de falhas associadas aos equipamentos utilizados (elementos de rede), com estimativa de sua frequência e duração. No trabalho apresentado nesta tese, buscou-se a identificação dos elementos críticos em redes ópticas, com base no impacto e no grau de risco relacionado às falhas desses equipamentos. Além de subsidiar possíveis análises financeiras sobre o impacto de falhas desses elementos, os resultados do modelo proposto fornecem suporte ao processo decisório relativo à escolha de pontos candidatos à redundância.

2.7 TRABALHOS RELACIONADOS

De acordo com Lazar (1992), as duas técnicas mais conhecidas para o problema de detecção e identificação de falhas em redes de telecomunicações são: método probabilístico e modelagem de redes como máquinas de estado finito. Basicamente, os métodos diferem no modelo da rede que é utilizado, na descrição dos canais estabelecidos, na entrada para o algoritmo, ou ainda, na metodologia do processamento das informações para a localização das falhas (BOULOUTAS *et al*., 1994; *et al*., 1997).

A maioria dos sistemas de filtragem é do tipo autossustentável ou está numa camada de um nível mais alto, portanto, trabalham GARDNER em conjunto com sistemas de gerenciamento de redes (LEE e CHO, 1998; LEHR *et al*., 1998) ou em camada acima desses sistemas (FUMAGALLI e VALCARENGHI, 2000). Para tratar do efeito de tempestade de alarmes, a *Hewllet Packard (HP)* desenvolveu os serviços de correlação de evento, *ECS (Event*

Correlation Services) (HP, 1995), que é um sistema baseado em regras e que possui uma arquitetura distribuída, o que permite a distribuição da correlação de eventos, contribuindo para reduzir o tráfego de informações de gerência na rede (HP, 1996). Um filtro modular que distribui por módulo a responsabilidade por cada segmento de rede e por uma certa funcionalidade é apresentado por Möller *et al*., (1995), onde uma implementação de filtragem inteligente que atua sobre um sistema de gerência de rede SDH é mostrada utilizando o paradigma de correlação baseada em regras. Modelos de comportamento foram utilizados para identificar problemas críticos, correlacionar alarmes e executar ações sobre a rede no sistema *Nerve Center Pro*, da Seagate (SEAGATE, 1996).A pesquisa de Brugnoni *et al*., (1993) apresentou o *Sinergia*, sistema especialista baseado em regras, utilizado no diagnóstico de falhas da rede de telecomunicações italiana, através de correlação em tempo real de alarmes das redes de transmissão e de comutação, reduzindo significativamente a quantidade de informações apresentadas aos operadores.

Atuando em cima do fluxo de alarmes produzidos por um sistema de telecomunicações, o *Analisador de Sequência de Alarmes de Telecomunicação, TASA (Telecommunication Alarm Sequence Analyzer)* (HATONEN *et al*., 1996), procura por regularidades, isto é, sequências de alarmes que ocorrem com certa frequência e, baseado nestes, propõe regras que podem ser incluídas em um sistema de correlação. Meira (1997) utiliza redes bayesianas para localizar falhas em redes de telecomunicações, a partir da correlação de alarmes. Em termos de objetos gerenciados em Fabrveniste *et al.,* (2004), todos os objetos são equipados com uma função de gerenciamento, a qual é responsável pela geração de alarmes. Os alarmes são emitidos quando ocorre uma falha local, ou em algum componente adjacente. O segundo caso é o que dá origem às propagações de falhas na rede. Em Sousa *et al*., (2005), nem todos os objetos gerenciados enviam alarmes (componentes passivos), somente os objetos gerenciados denominados de componentes alarmantes possuem essa função. Esses são divididos em dois grupos: um que envia alarmes próprios e um outro que envia alarmes quando algum componente da rede adjacente falha.

De acordo com Benhcine *et al*., (2013), a resiliência da rede tornou-se um dos maiores requisitos do provedor de serviços para implantar aplicativos em tempo real e atender às necessidades de qualidade de serviços (*QoS*) do cliente. O trabalho teve foco em um dos mecanismos de proteção recentemente desenvolvidos para a camada 3 (rede). Os provedores de serviços tendem a se beneficiar da flexibilidade da rede IP / MPLS para implementar serviços

de ponta a ponta com garantias de *QoS* elevadas. Entretanto, os mesmos exigem um tempo de proteção o mais próximo possível das redes baseadas em SONET. O trabalho apresentou um teste experimental de *Fast Reroute* em rede real. Foi avaliado o tempo de perda e o tempo de convergência após a falha do *link* em diferentes cenários com *Fast Reroute* ativado. Os resultados mostraram que *Fast Reroute* pode fornecer um nível de proteção que satisfaça o requisito de provedores de serviços e principalmente o requisito de transmissão em tempo real. No entanto, a eficiência de proteção *Fast Reroute* foi afetada com o tamanho da rede, onde o tempo de perda aumenta à medida que o tamanho da topologia da rede aumenta.

Foi apresentado em Sterbenz *et al*., (2010) uma arquitetura sistemática quadro que unifica disciplinas de resiliência, estratégias, princípios e análises. A regra consistia em defender, detectar, corrigir, recuperar + diagnosticar, refinar (D2 R2 + DR). A estratégia *ResiliNets* conduz a um conjunto de princípios de *design* que orientam a análise e *design* de redes resilientes. Os princípios abrangem pré-requisitos, compromissos, habilitadores e comportamentos para arquiteturas e projetos de redes resilientes. Em Smith *et al*., (2011), é descrito uma abordagem sistemática da resiliência da rede. Os aspectos desse trabalho representam uma visão de resiliência a mais longo prazo e exigem mudanças mais radicais na forma como os operadores de rede atualmente pensam sobre a resiliência.

A redundância de ativos em uma arquitetura de rede pode exigir a pré-reserva ou duplicação de alguns recursos da rede, que devem ser planejados em conjunto com a fase de projeto da rede. A presente pesquisa busca a identificação de pontos de redundância em redes existentes que possuam algum histórico de falhas, que possa ser utilizado como base das entradas para as simulações pelos gestores.

Qualquer investimento em redundância deve gerar algum tipo de retorno para a empresa. Enquanto investimentos com retornos superiores ao custo de capital aumentam o valor da empresa; investimentos com retornos inferiores ao custo de capital, reduzirão esse valor.

A maioria dos algoritmos de redundância são projetados para indicar redundância em seções de rede, ou seja, envolvem todo o *link* de comunicação. Dessa forma, a identificação de pontos de redundância torna-se mais complexa e muitas vezes cara. O trabalho de Finn *et al*., (1998) mostra um algoritmo *APS* do tipo de rede *Bidirectional Links SELF-healing* (BLSN) que cria dois subgrafos direcionados totalmente conectados à rede. Esses subgrafos são construídos de tal forma que, após o nó ou a borda falhar, todos os nós operacionais ainda estão

conectados pelo subgrafo. Existe um caminho de *backup* para qualquer falha na borda e foi implementado um nó de recuperação de falhas.

Em Ḿedard (1999), foi apresentado um algoritmo que cria árvores redundantes em redes arbitrárias com nó redundante ou *link* redundante. No caso de falha de um nó ou *link*, qualquer nó está conectado à raiz dessas árvores em pelo menos um dos ramos e o esquema prevê uma rápida recuperação pré-definida de comunicações, com grande flexibilidade no *design* da topologia (algoritmo fornece um superconjunto de árvores anteriormente conhecidas). As soluções apresentadas diferem da discutida nesta tese porque o risco não foi modelado.

Homma *et al*., (2016) apresentou um método de recuperação de falhas, utilizando estruturas de anel denominadas *tie-sets*, propondo um algoritmo que pesquisava um grupo de *tie-sets* que gera um caminho de desvio mais curto no caso de uma falha de *link*. Os autores idealizaram *tie-sets* com base na teoria dos grafos, dividindo uma rede de malhas em *loops* lógicos, gerenciando as falhas com os mesmos.

De acordo com Li-xia e Yue-Jin (2014), as redes *ethernet* ópticas passivas orientadas a conexão (EPONs) incluem em sua arquitetura funcional, o gerenciamento de falhas e a criação de uma rede de mecanismos de proteção automática para testar a função dos testes de simulação e a proteção de seus programas originais. A aplicação desse método pode fornecer uma proteção automática e rápida para atender requisitos de capacidade de sobrevivência da rede de transmissão.

Saste *et al*., (2016) afirmam que a *Operação, Administração e Manutenção (OAM)* consiste em um conjunto de ferramentas com a finalidade de gerenciar diferentes camadas de rede, podendo detectar e isolar as falhas e ainda realizar o monitoramento de desempenho de uma rede, contribuindo assim para a redução do custo operacional. Os autores afirmam que o mecanismo *OAM* é importante para redes que são necessárias para oferecer objetivos de desempenho e disponibilidade. O conjunto de ferramentas OAM é definido para diferentes camadas na pilha de protocolos. Uma vez que muitos organismos padrão estão trabalhando no aprimoramento do OAM, existem vários padrões executando a mesma funcionalidade. O trabalho apresentado detalhou um conjunto de ferramentas *OAM* disperso das redes *Ethernet, MPLS e IP*, propondo uma solução para a convergência desse conjunto de ferramentas, gerando assim benefícios para o provedor de serviços e o cliente.

Um algoritmo de localização de falhas (AFA-FLA) foi recomendado em Mas *et al.,* (2000). Em Sousa *et al*., (2005), foi apresentado um algoritmo para localização de falhas e cuja principal vantagem em relação a outros algoritmos era a pequena quantidade de informações necessárias para localizar as falhas. No entanto, a solução proposta não abordou os riscos inerentes ao negócio de falhas identificadas. A pesquisa proposta nesta tese utiliza o conceito de domínio de alarmes (SOUSA *et al*., 2005) como base conceitual para o desenvolvimento do modelo proposto. O gerador de domínio monta, para cada elemento dado da rede pertencente à via física, o conjunto de elementos que enviará alarmes se um dado elemento falhar. Tipos variados e quantidades de alarmes podem ser emitidos para o gerenciamento. Esta variação dependerá fundamentalmente de dois fatores: a posição em que o componente está no canal e o número de canais que o atravessam.

Foi identificada uma necessidade de se desenvolver e manter o controle sobre as interdependências entre as infraestruturas de rede. Uma abordagem baseada em risco para proteger infraestruturas de rede críticas foi apresentada em Bloomfield *et al*., (2017). Os autores argumentam que os gerentes de infraestrutura de rede precisam estar cientes do impacto das interrupções em outras infraestruturas de rede em relação aos serviços, para desenvolver planos de contingência que possam atenuar o risco. Foi apresentado um método sistemático chamado *Análise Preliminar de Interdependência* (PIA), que buscou apoiar o desenvolvimento de modelos para o tratamento de infraestruturas complexas, críticas e interdependentes (LCCIs).

O projeto de redes ópticas metropolitanas inteligentes foi apresentado e comparado com algumas abordagens tradicionais em Fen *et al*., (2016). Os autores afirmam que a construção de redes ópticas metropolitanas inteligentes permite que os serviços de configuração e modificação sejam mais rápidos e mais convenientes para resolver problemas. A sobrevivência empresarial e a expansão da rede são melhoradas por uma rede flexível. A utilização da largura de banda é melhorada a partir de uma variedade de pontos de proteção e restauração focados em negócios, resistindo a múltiplos pontos de falha de maneira efetiva.

O modelo proposto (*ASP*) é semelhante ao modelo usado em Oliveira *et al*., (2003), trabalhando com um detector de falhas que possui conhecimento sobre quais componentes podem ter falhado. O detector pode cometer erros (por exemplo, pode suspeitar de componentes que funcionam corretamente), mas a lista de componentes suspeitos é pequena o suficiente para permitir uma identificação rápida do componente que causou a falha. Oliveira *et al*., (2003) afirma que a monitoração da rede ocorre para qualquer falha potencial, e quando uma falha

potencial é detectada, um ou mais componentes que parecem estar com defeito são identificados. A probabilidade de sucesso e / ou impacto potencial determina ações de mitigação adequadas. O trabalho em Oliveira *et al*., (2003) se relaciona com a presente pesquisa, porque mostra uma tecnologia que considera o impacto da rede e mitiga automaticamente as falhas do centro de dados, em vez de confiar na intervenção humana para diagnosticar e reparar a rede. O foco da presente pesquisa foi a identificação dos pontos de redundância em redes ópticas, com base na avaliação de risco. Os conceitos que envolvem estimativa de risco e seu impacto no modelo e ferramenta de *software* propostos são simples, fáceis de usar pelos gerentes e podem fornecer suporte ao processo de tomada de decisão.

O trabalho apresentado em Fabrveniste *et al*., (2004) se relaciona com a presente pesquisa, pois prevê situações de falha em um *link* óptico (que simula a camada física com transmissor, receptor e fibra óptica). Além de considerar os componentes no *link* óptico mencionados por Fabrveniste *et al*., (2004), o algoritmo *ASP* proposto neste trabalho também funciona com o demultiplexador, o multiplexador, o interruptor de proteção, o *switch*, o filtro de derivação e inserção e a porta de acesso local. Com a adição desses componentes, os resultados obtidos com o uso do *ASP* servem para lidar com situações em ambientes reais.

Da Silva e Fagotto (2014) afirmam que os esforços na literatura se concentram em potencializar a disponibilidade da rede e dos serviços nela contidos, bem como prover um rápido reestabelecimento da mesma em caso de falhas. A proposta dos autores teve como foco mais geral o acompanhamento executivo (com base nos processos) em crises decorrentes de incidentes em tais ambientes, através de proposta de fluxo para uma estrutura de atendimento que aplicasse processos integrados com as melhores práticas.

A pesquisa apresentou um método para a classificação, diagnóstico e tratamento dos incidentes a partir de processos para rastreamento de problemas na rede buscando a identificação dos ambientes críticos ao negócio. Da Silva e Fagotto (2014) procederam avaliação do processo de gerenciamento de incidentes relativo aos serviços de gerenciamento de rede de uma empresa global para 68 empresas clientes de diversos tamanhos e objetivos de negócio. Os resultados indicaram que 56% dos principais problemas de redes (observados na volumetria) se concentravam em apenas 2 categorias entre problemas analisados. As causas primárias dos eventos mais relevantes foram analisadas. A causa primária é a razão pela qual um evento de problema ocorreu, como um erro operacional, uma falha de energia, etc. As

Figuras 28 e 29 mostram que os registros de problemas de *switch* e *link* ocorrem com maior frequência e as principais causas identificadas.

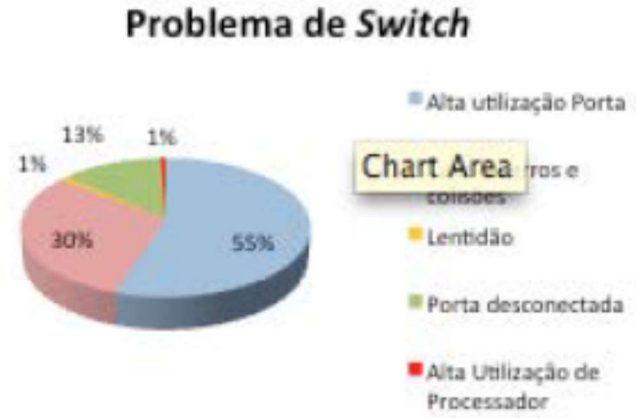


Figura 28. Causas primárias dos problemas de Switch.
Da Silva e Fagotto (2014).

Figura 29. Causas primárias dos problemas de Link.
Da Silva e Fagotto (2014).

Em uma abordagem diferente, a presente pesquisa teve como foco a identificação de pontos passíveis de redundância em redes ópticas, através de simulações de cenários, com base no risco para o negócio. O problema abordado envolve a promoção de alinhamento entre TI e negócio na atividade de suporte a tomada de decisão, abrangendo os níveis operacional e estratégico. Nesta pesquisa, buscou-se observar o atendimento dos requisitos para modelagem em *Business-driven IT Management (BDIM)* (BARTOLINI, 2009), com a proposição de modelos não intrusivos, que possam ser considerados úteis e simples pelos gestores.

De acordo com Thyagaturu *et al*., (2016). o paradigma das redes definidas por software (*software defined networking* - *SDN*) separa o plano de dados do plano de controle e centraliza

o controle da rede em um controlador *SDN*. As aplicações interagem com controladores para implementar serviços de redes, tais como transporte de rede com qualidade de serviço. O uso de *SDN* facilita a virtualização das funções de rede de tal forma que múltiplas redes virtuais podem operar sobre uma dada infraestrutura física de rede. Devido a características específicas dos componentes de comunicação óptica e das altas capacidades de transmissão óptica, as redes ópticas baseadas em *SDN* possuem desafios específicos, porém possuem um grande potencial. O trabalho dos autores pesquisou estudos sobre o paradigma *SDN* em redes ópticas, aos níveis de infraestrutura, controle e aplicação.

Avanços recentes nas técnicas de transmissão de fibra óptica, tais como a transmissão óptica por multiplexação coerente por divisão ortogonal de frequência (*CO-OFDM*) e *Nyquist-WDM* permitem a transmissão de um canal ótico em diferentes formatos de modulação e larguras de banda. Foi possível se construir uma nova geração de redes ópticas onde a utilização da largura de banda é consideravelmente mais flexível do atualmente, ou seja, redes ópticas elásticas flexíveis (*EONs*). Shen *et al*., (2016) afirmam que as redes ópticas elásticas (*EONs*) têm recebido ampla atenção devido à sua flexibilidade inerente e à eficiência com que alocam a largura de banda de fibra. Para uma *EON*, a capacidade de sobrevivência é de vital importância devido à grande largura de banda que carrega em cada canal ótico. Os autores analisaram o estado atual da arte dos *EONs* sobreviventes, procedendo uma revisão de literatura, visando resumir os seguintes aspectos: (a) compartilhamento de recursos de espectro entre *lightpaths* de backup, (b) compartilhamento de *transponders* óticos de alta velocidade, (c) efeito de conversão de espectro, (d) restauração de largura de banda comprimida (*BSR*), (e) restauração conjunta por múltiplos canais óticos de sub-faixa, (f) capacidade de sobrevivência de várias camadas e (g) eficiência energética. Além de um resumo sobre o status atual da pesquisa, foram discutidas questões abertas de pesquisa em *EONs* sobreviventes, sob a perspectiva de (a) impacto da conversão do espectro, (b) impacto da configuração elástica do *transponder* ótico, (c) impacto das deficiências e limitações da camada física, (d) desfragmentação de espectro baseada em caminho de proteção e (e) disponibilidade de rede. Os autores revisaram o estado da arte sobre *EONs* sobreviventes, abordando as futuras questões de pesquisa para esse tipo de rede.

De acordo com Gomes *et al*., (2013), assegurar a sobrevivência da rede é de extrema importância nas redes atuais. Um *Grupo de Links de Risco Compartilhado* (SRLG) é o conjunto de *links* na rede que compartilham um recurso físico comum sujeito a falha(s). Este conceito permite uma camada superior a capacidade de implementar o roteamento diversificado da

SRLG. Dois algoritmos, *Conflicting SRLG Exclusion (CoSE)* e *Iterative Modified Surballe's Heuristic (IMSH)*, foram revistos no trabalho apresentado. O primeiro resolve o problema *min-min* e o segundo problema da *min-sum*, considerando os caminhos disjuntos de *SRLG*. Foi descrita uma nova versão do *CoSE*, denominada *CoSE-MS*, visando resolver o problema da *min-sum* para o roteamento diversificado da *SRLG*. O desempenho do *CoSE-MS* e *IMSH* foi comparado por meio do uso de redes aleatórias e uma rede óptica.

3 ASPECTOS METODOLÓGICOS

3.1 METODOLOGIA DE PESQUISA

O modelo proposto tem como uma de suas bases conceituais os processos de gerenciamento de incidentes e falhas do ITIL (OGC, 2007), propondo uma gestão proativa no que se refere à mitigação das falhas mais críticas, sob o ponto de vista de planejamento estratégico, possibilitando assim o desenvolvimento de uma abordagem que interaja melhor com o planejamento de negócio, considerando as variáveis que influenciarão a tomada de decisão sobre possíveis pontos de redundância em rede ópticas. Conforme mostrado na Figura 30.

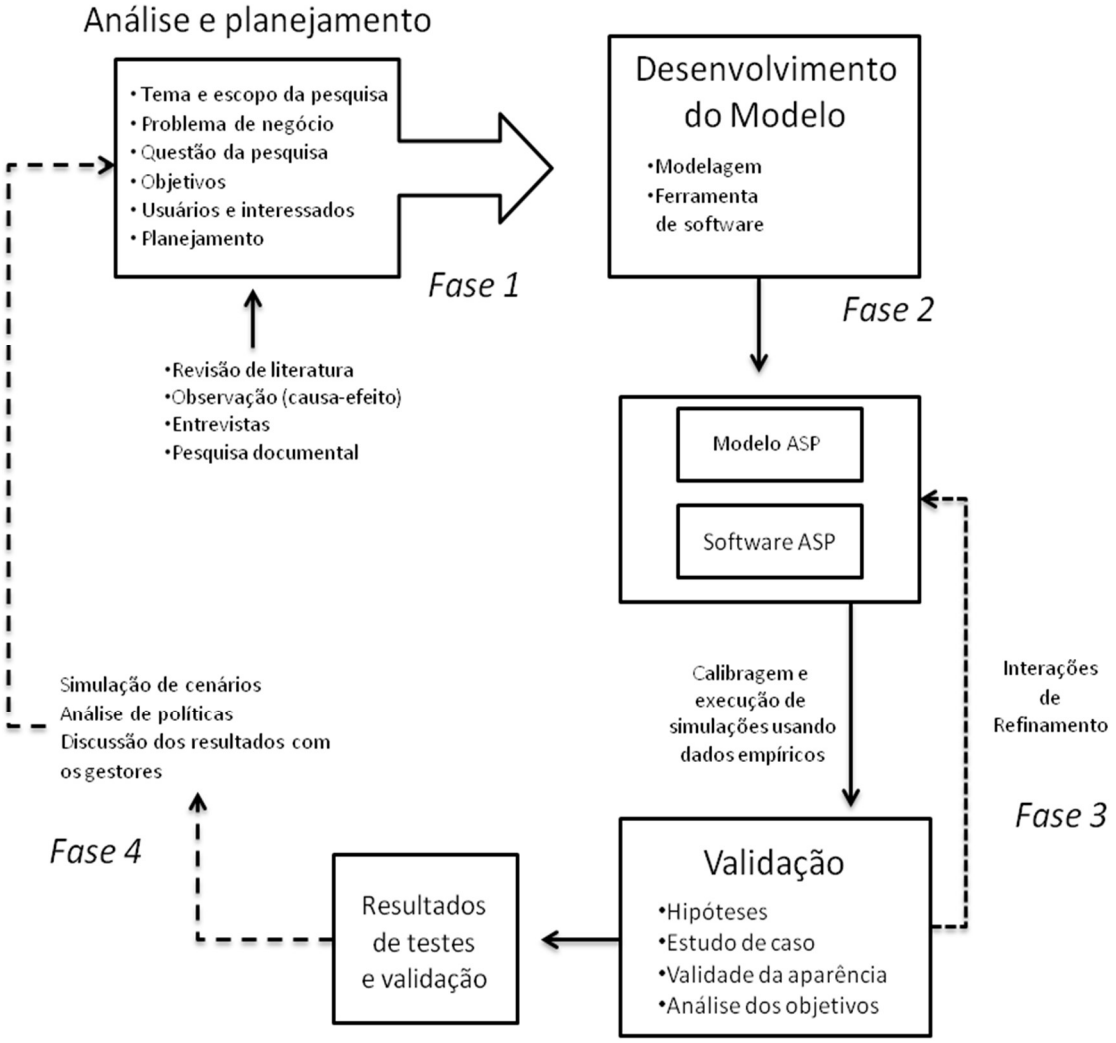


Figura 30. Desenho da pesquisa. Elaborada pelo autor.

A pesquisa apresentada nesta tese foi realizada em quatro fases iterativas. Na primeira fase, foram delimitados o tema e escopo da pesquisa, o problema de negócio que envolve a necessidade de identificação de pontos de redundância em redes ópticas na visão do negócio, os objetivos, bem como a definição dos interessados. Foi realizada revisão de literatura, observação na empresa avaliada, com a realização de entrevistas e pesquisa documental *in loco*. Durante a fase de planejamento, a ideia foi amplamente discutida e ao final foi validada pelos gestores.

A segunda fase do trabalho envolveu o desenvolvimento do *modelo ASP*, bem como sua implementação em uma *ferramenta de software*, também denominada *ASP*. Foram realizadas interações para refinamento do modelo, bem como várias sessões de simulações, visando a calibragem e validação da ferramenta, a partir de dados empíricos.

A terceira fase do trabalho apresentado envolveu a execução de cinco simulações de cenários de redes ópticas de referência, com a participação de gestores no processo de validação, conforme será descrito na sequência. A partir das hipóteses elencadas, foi realizado um exercício de validade de aparência (RUNERSON e HOST, 2009).

De acordo com Bezerra (2015), a simulação é uma simplificação do mundo real e, portanto, é inerentemente uma aproximação. Simuladores (ou modelos de simulação) precisam passar por um julgamento que aprove ou reprove a sua utilidade. A validação visa testar a corretude externa do modelo, ou seja, se ele é apropriado para atacar o problema alvo, requerendo conhecimento especializado sobre o sistema real.

Segundo Barlas (1989), a validação de um modelo pode ser definida como "estabelecer confiança na utilidade do modelo com respeito ao seu propósito". O processo de validação deve se preocupar com a criação de confiança suficiente em um modelo de simulação para que os seus resultados sejam aceitos pelos usuários e patrocinadores (*stakeholders*). Isso pode ser feito tentando-se provar que o modelo está incorreto. "Quanto mais testes forem realizados nos quais não se pode provar que o modelo está incorreto, mais aumenta a confiança no modelo" (MORECROFT, 2007).

Os resultados obtidos foram analisados e discutidos com os gestores da empresa, em sessões que envolveram a análise de políticas, utilidade a aplicabilidade do modelo para a

empresa em cenários reais. Os gestores responderam a questionários, bem como foram realizadas entrevistas semiestruturadas com os mesmos, relativas à validação das hipóteses de pesquisa, bem como sobre o atingimento dos objetivos deste estudo.

3.1.1 Pesquisa bibliográfica e validação com a comunidade acadêmica

Após uma extensa pesquisa bibliográfica sobre os temas relacionados com esta tese de doutorado, o primeiro passo incluiu a definição de um processo para suportar a tomada de decisão relacionada à identificação de pontos críticos, passíveis de redundância em redes ópticas. Após a execução do estudo de caso, os dados obtidos foram confrontados com informações da revisão de literatura e das observações realizadas, em processo de triangulação. O estudo de caso realizado foi planejado, desenvolvido, testado e validado, em consonância com as recomendações de Runerson e Host (2009).

A obtenção de validação da pesquisa por parte da comunidade acadêmica foi um dos focos desta tese. Visando a obtenção de um retorno sobre a proposta desta tese, a presente pesquisa foi apresentada, tendo obtido um artigo aceito para publicação na revista *IEEE Latin America Transactions* e se encontra com um artigo em processo de avaliação para publicação na revista *IEEE Transactions on Network and Service Management*. As duas revistas possuem uma boa qualificação na área de *Engenharias IV*, a qual pertence o *Programa de Pós graduação em Engenharia de Teleinformática-PPGETI*.

3.2 ORGANIZAÇÃO PARTICIPANTE

Durante o estudo realizado, foi selecionada uma empresa no estado do Ceará, com base nos seguintes critérios de escolha:

1. Permissão de acesso do pesquisador aos seus dados e informações históricas quanto aos registros referentes à utilização dos serviços de TI e redes ópticas.

   Conveniência em relação à facilidade de acesso do pesquisador às dependências da área de TI.

2. Acesso ao planejamento estratégico da organização.

3. Transparência da organização em mostrar seu nível de maturidade quanto a utilização de *frameworks* de mercado e iniciativas para organização e gestão da TI.
4. Facilidade de interação e relacionamento com os gestores de TI da empresa enquanto pesquisador e aluno de doutorado em Engenharia de Teleinformática pela Universidade Federal do Ceará.

3.3 HIPÓTESES DE PESQUISA

Responder à questão de pesquisa formulada envolve validar o uso do modelo proposto nesta tese por tomadores de decisão (gestores) especialistas em gerenciamento de serviços de TI, no que se refere ao processo de gerenciamento de falhas em redes de computadores ópticas. Para contribuir com este esforço, quatro hipóteses foram investigadas:

- **Hipótese 1 (H1)**: O modelo proposto é útil para os gestores.
- **Hipótese 2 (H2)**: O modelo proposto é preferível em relação às abordagens atuais utilizadas.
- **Hipótese 3 (H3)**: O modelo proposto é completo para a identificação de pontos críticos passíveis de redundância em redes ópticas.
- **Hipótese 4 (H4)**: O modelo proposto é efetivo/eficaz para suportar os processos de gerenciamento de incidentes e falhas.

O objetivo fundamental do estudo de caso realizado consistiu na verificação das hipóteses formuladas, por meio da análise sobre os resultados coletados durante sua execução.

Por efetivo compreende-se:

- é capaz de identificar pontos críticos em redes ópticas;
- é capaz de expressar os conceitos de impacto e risco de elementos de redes ópticas, o que permite a comparação de dois ou mais itens representados pelo modelo com base no risco de cada item;
- os resultados apresentados pelo modelo são consistentes e objetivos o bastante para basear a tomada de decisão na escolha de pontos candidatos a redundância; e

- os resultados obtidos da aplicação do modelo são compatíveis com os resultados de outros métodos que apoiam o processo de tomada de decisão.

3.4 ETAPAS DA PESQUISA

Foi necessário um esforço de compartilhamento de conhecimento junto aos atores envolvidos nesta pesquisa, como forma de alinhar as expectativas e os resultados do modelo *ASP*. Foram realizadas entrevistas semiestruturadas com os gestores de rede e da área de tecnologia da informação da empresa *Alpha*. Os gestores tiveram acesso a todo o referencial teórico que fundamenta o modelo *ASP*, bem como participaram das simulações de cenários realizadas. A Tabela 7 apresenta as fases que envolveram o estudo de caso realizado.

Tabela 7 - Envolvimento de gestores/empresas nas fases da pesquisa

Fase	Atividades realizadas
1	Apresentação dos principais conceitos da pesquisa
	Entrevista de aquisição de conhecimento (definição do problema, identificação do objetivo do modelo)
	Pesquisa documental – Processos de gerenciamento de serviços de TI/Redes
	Reunião de validação e verificação (problema, objetivos do modelo)
2	Execução do *primeiro cenário simulado*
	Execução do *segundo cenário simulado*
	Execução do *terceiro cenário simulado*
	Execução do *quarto cenário simulado*
	Execução da *quinta simulação - segunda proposta de cálculo do impacto de um elemento de rede*
	Análise das simulações realizadas
3	Apresentação e discussões para avaliação e validação do modelo *ASP*

4	Aplicação de formulário (questionário) para avaliação das hipóteses de pesquisa sobre o modelo pelos gestores da empresa pesquisada. Realização de entrevistas semiestruturadas.

3.5 PESQUISA DOCUMENTAL

Durante o estudo de caso realizado, a verificação quanto a adoção de modelos de gestão e utilização de *frameworks* para apoio e organização das atividades de gerenciamento de serviços de TI (com foco na gestão de redes) foi uma importante fonte de conhecimento a ser incorporada à pesquisa. Através da observação, verificação e entrevistas com os gestores, foi identificada a necessidade da empresa avaliada aprofundar e aplicar mais efetivamente as recomendações dos guias de melhores práticas (ITIL, COBIT). Percebeu-se as seguintes dificuldades na empresa avaliada:

- Ausência de um modelo de gestão estratégica mais completo para a empresa e baixa adesão na utilização de *frameworks* de boas práticas;
- Dificuldade em executar as ações em conformidade com o que foi planejado;
- Pouca documentação dos processos. Não seguir os processos definidos em alguns casos.

Houve total disponibilidade dos gestores para subsidiar as informações demandadas durante o estudo de caso, porém, a empresa avaliada apresentou ausência de diversos documentos que poderiam apoiar o levantamento de informações realizado.

3.6 AMEAÇAS À VALIDADE

Foram identificadas as seguintes ameaças à validade da pesquisa realizada:

- o estabelecimento de uma relação direta entre a quantidade de alarmes, relevância do elemento de rede para o negócio e impacto do reparo no cálculo do valor esperado do risco (*ERV*) consiste em um risco, apesar dos fortes indícios e da identificação de elementos na literatura que forneceram suporte à proposta. A

flexibilidade do modelo nesse quesito transfere a responsabilidade da proposição de novas formas de cálculo do impacto de um elemento de rede para os gestores;

- para se ter uma validação estatística através de estudos de caso, seriam necessários mais testes em diferentes empresas e cenários, o que não foi possível na janela de tempo disponível para a realização do trabalho. Entretanto, as simulações realizadas foram validadas em termos estatísticos, conforme implementação no *software ASP*;
- apesar da avaliação de ameaças externas ter indicado que não é difícil generalizar os resultados do experimento, existe um risco nessa generalização, já que não foram realizados testes exaustivos nesse sentido;
- e pela natureza do modelo proposto e das diferentes complexidades dos cenários de negócio, algumas informações são obtidas dos atores envolvidos, existindo o risco de obtenção de informações falsas ou incorretas (decorrente de erros).

4 MODELO PROPOSTO

Este capítulo descreve o modelo *ASP*. São apresentados os detalhes de sua contextualização e os resultados que podem ser obtidos através da sua utilização pelos gestores. O ambiente de rede óptica do modelo *ASP* foi baseado em Sousa *et al*., (2005). Para o desenvolvimento do modelo proposto, foram considerados os seguintes dispositivos óticos e optoeletrônicos:

1. **Fibra óptica**: é um dispositivo passivo e não envia qualquer tipo de alarme.
2. **Transmissor (TX):** Toda vez que o TX passa de um regime de trabalho para outro, um alarme é enviado. Isso pode acontecer, por exemplo, se o controle de temperatura do laser não estiver funcionando corretamente. No entanto, se o transmissor começar a funcionar em um regime não permitido, para segurança, o TX é desligado automaticamente e um alarme é enviado para a sala de gerenciamento.
3. **Receptor (RX)**: O receptor envia um alarme para a sala de gerenciamento quando a potência óptica de entrada está abaixo de um valor especificado.
4. **ADD / Drop Filters (ADF):** são responsáveis pela inserção (derivação) de um comprimento de onda em (a partir de) um sinal composto por vários comprimentos de onda. Quando o ADF não está funcionando corretamente, ele envia um alarme para a função de gerenciamento.
5. **Amplificador 3R:** um alarme é enviado para a sala de gerenciamento quando não é possível recuperar o sincronismo do sinal de entrada.
6. **Proteção da Switch (PS):** quando o sinal escolhido como comprimento de onda de referência não possui potência óptica suficiente, o PS escolherá outro sinal de entrada com potência óptica aceitável e um alarme será enviado para a função de gerenciamento.
7. **Switch (SW):** quando mostra mau funcionamento, envia um alarme para a função de gerenciamento.
8. **Multiplexador / Demultiplexador:** é um dispositivo passivo e não envia qualquer tipo de alarme.

Os componentes capazes de enviar alarme estão nos seguintes grupos (SOUSA *et al*., 2005):

• ***Self-Alarmed***- Componentes de rede que podem enviar alarme aos gerentes quando eles próprios não estão trabalhando legitimamente. Este tipo de componente é considerado pertencente à categoria A1 ou A3;

• ***Out-Alarmed***- Componentes de rede que podem enviar alarmes quando ocorre algum evento externo, ou seja, eles enviam alarmes para gerenciadores informando uma condição anormal em algum ponto do canal, mesmo quando não são responsáveis pelo problema. Esses componentes pertencem à categoria A2;

• ***Failure Masking***: os componentes do grupo podem ocultar os alarmes enviados pelos componentes anteriores, uma vez que o canal é uma sequência ordenada de componentes. Esses componentes pertencem à categoria A3.

No modelo proposto, um nó utiliza um comprimento de onda alternativo e uma associação física entre dois nós possui duas fibras, uma para cada direção de comunicação. Uma atividade de informação encaminhada para um determinado nó pode alcançá-lo através de pelo menos dois caminhos distintos e um interruptor de proteção decidirá qual deles será usado de acordo com seu nível de potência óptica. Os nós são classificados como nós centrais ou nós locais. Uma vez que um nó central possui um *Switch*, pode proceder uma comutação entre diferentes comprimentos de onda. Um nó central pode ao mesmo tempo ser conectado a alguns nós diferentes e um nó local é retratado pela proximidade de um filtro *ADF* e pode ser vinculado a dois nós diferentes.

Cada componente de rede possui uma identificação única, utilizada na identificação de qual componente de rede está danificado e a qual nó pertence, na ocorrência de uma falha. Essa identificação é composta por uma sequência de quatro campos (A, B, C, D), com o seguinte significado para um nó local:

A: indica a categoria e pode assumir os seguintes valores: 0 - componente não Outalarmed; *1 - Selfalarmed; 2 – Out-alarmed; 3 – Failure masking*.

B: indica o número do nó.

C: é sempre 0 para um nó local.

D: identifica a posição do componente dentro do nó. Os valores deste campo variam de acordo com o componente: LAP = 0 (Local Access Port); ADF = 1 ou 2; RX = 1 ou 2; Amplificador 3R = 4 ou 5; TX = 5 ou 6; PS = 3.

O *kernel* do modelo de rede é a conexão entre componentes que podem alarmar ou não. O modelo *ASP* possui capacidade para encontrar componentes passivos danificados, precisando apenas da identificação dos elementos que estão enviando alarmes. A correlação de alarme empregada reduz a quantidade de componentes de rede suspeitos, que varia de acordo com o número de canais que utilizam o componente danificado. Um maior número de canais melhora a eficiência e a precisão do algoritmo. O processamento automático da relação de localização alarme / falha realizada pelo algoritmo reduz também o tempo necessário exigido pela solução completa do problema. O modelo proposto identifica os elementos da rede em relação à sua relevância comercial e estima o valor do risco para cada ponto crítico. Assim, o modelo *ASP* é eficaz na identificação dos elementos mais críticos da rede óptica. Os gerentes podem decidir quais serão os pontos de redundância da rede, a partir da visão do negócio.

4.1 ASPECTOS DE MODELAGEM

4.1.1 Escopo do modelo

A presente pesquisa envolveu uma triangulação entre revisão de literatura, observação e realização de estudo de caso, visando a validação do modelo proposto. Foram realizadas entrevistas exploratórias com gestores de TI, redes e analistas de infraestrutura de empresas do estado do Ceará. Buscou-se o entendimento do processo de gerenciamento de falhas em redes ópticas, com foco na visão do negócio, sob a óptica dos guias de melhores práticas ITIL, COBIT, PMBOK e ISO/IEC 27002.

Os resultados obtidos podem subsidiar decisões que favoreçam a escolha de pontos de redundância em redes ópticas, mitigando o risco de falhas, e assim ajudando os provedores de serviços a alcançarem os seus objetivos estratégicos.

O entendimento do processo de gerenciamento de falhas influencia no desempenho das atividades, podendo levar a melhores resultados e decisões com relação a investimentos em recursos. Diante desse fato, o escopo do modelo *ASP* pode ser dividido em três partes:

1. Analisar os serviços de redes ópticas, com o propósito de dar suporte aos gestores de TI para entendimento da identificação de pontos críticos candidatos a redundância e na tomada de decisão sobre gestão de serviços em redes ópticas;
2. Possibilitar o entendimento e compreensão dos serviços de redes óptica sem relação ao alcance de objetivos específicos de TI;
3. Considerar o relacionamento, causa e efeito, entre os objetivos da TI com os objetivos do negócio, nas atividades que envolvem o gerenciamento de incidentes e de falhas em redes ópticas.

4.1.2 Delimitações do modelo

Com o objetivo de explicitar com maior clareza o objeto de estudo, as seguintes delimitações foram adotadas:

- Foco na gestão de redes ópticas da organização pesquisada. Dentre as várias categorias de recursos de TI, a pesquisa considera os recursos e elementos de redes (critérios quantitativos e qualitativos);
- Foco na execução dos processos de Gerenciamento de Falhas e Gerenciamento da Incidentes;
- Foco nos objetivos estratégicos da TI, do Negócio e no relacionamento entre eles;
- Foco na gestão de riscos envolvida no processo de gerenciamento de falhas em redes ópticas.

4.2 DESCRIÇÃO DO MODELO

4.2.1 Visão geral

Existem quatro etapas para a execução do modelo *ASP*:

1. Geração do domínio da rota física (biblioteca, topologia e canais) com os dados de entrada. No domínio da rota física, todos os elementos pertencentes a qualquer canal serão listados, e cada componente será associado ao(s) componente(s) que enviará alarme (s) ao gerenciamento se eles falharem;
2. A partir da análise das posições dos elementos dentro dos nós locais e centrais, e dos parâmetros de calibragem do modelo, é gerada a tabela de nível de impacto dos elementos;
3. Com a probabilidade de falha de cada elemento e os dados da tabela de nível de impacto, em conjunto com o domínio da rota física, o modelo estima o ranking de risco da rede;
4. O *ranking* de risco de rede do passo 3 é utilizado para indicar pontos de rede críticos. Desta forma, pode-se compreender de forma rápida e precisa quais pontos devem ser priorizados para possíveis investimentos.

A Figura 29 mostra o diagrama funcional do modelo ASP. A partir das informações de fluxo, é possível observar que o modelo possui quatro entradas (representadas por setas largas sombreadas em cinza na Figura):

1. **Biblioteca** - Coleção de modelos de componentes de rede, contendo o comportamento e a descrição de cada componente;
2. **Topologia** - descrição da composição e estrutura física dos elementos na rede;
3. **Canais** - conjunto de elementos de rede que estão se comunicando, de acordo com a topologia adotada, e que pode ser definido como uma lista ordenada de componentes;
4. **Valores de Probabilidade de Falha** - Estimados para cada tipo de elemento de rede.

Diferentes tipos e quantidades de alarmes podem ser emitidos para o gerenciamento. Esta variação dependerá fundamentalmente de dois fatores: a posição na qual o componente está no canal e o número de canais que o atravessam. É possível extrair o impacto comercial de cada

componente de rede a partir dos dados do gerador de domínio. É utilizada a *Probabilidade de Falha de Elemento(PF)*, cujo valor é multiplicado pelo grau de impacto para obter o *valor esperado do risco (ERV)* de cada elemento. Cada *ERV* de um componente de rede é apresentado como uma saída para o gerente em uma *interface* gráfica de usuário (GUI), através de tabelas ou gráficos para ajudar no processo de identificação de pontos críticos (Figura 31).

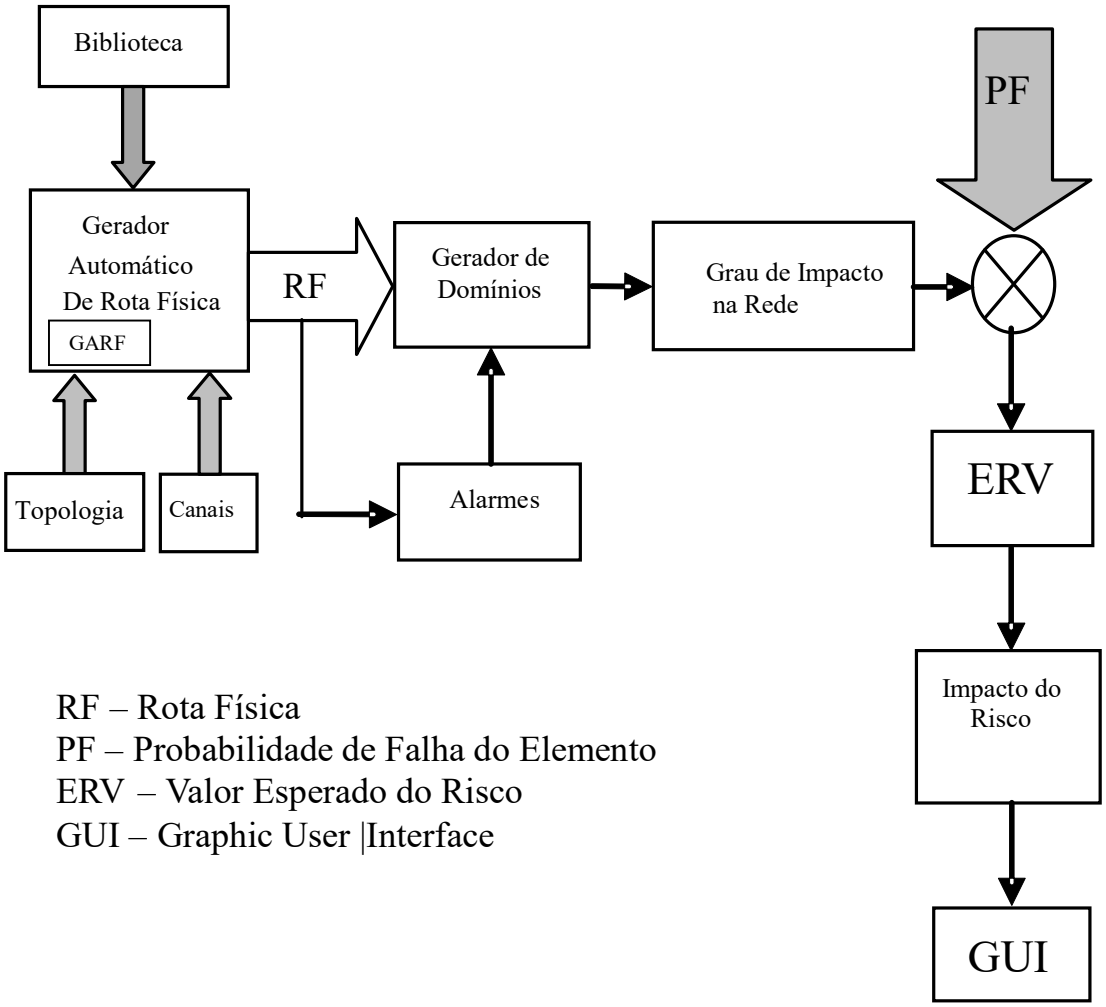


Figura 31. Diagrama funcional do modelo *ASP*. Elaborada pelo autor.

Umas das fases primordiais do processo é a localização de falhas. Descrição detalhada a seguir.

As três primeiras entradas são usadas pelo *Gerador de Rota Física Automática* (GARF) para produzir a rota física em sua saída. Na rota física, todos os canais são descritos, um componente por vez, ao contrário da informação fornecida na entrada, que indica apenas os nós do canal. A partir da RF, o conjunto de *Alarmes* é criado (neste conjunto, haverá a identificação

de cada componente de rede que pode enviar um alarme e a condição anormal associada).

O modelo *ASP* (Figura 32) contempla um simulador denominado de gerador automático de alarmes, recebendo como dados de entrada: a identificação dos elementos que deverão falhar, as saídas do gerador automático de rota física e as informações sobre a quantidade de alarmes falsos e perdidos. Na saída do simulador será apresentado um conjunto de alarmes - identificação dos componentes que enviarão alarmes, caso ocorra alguma falha nos elementos que foram indicados na entrada do simulador. Em seguida, o selecionador de alarmes fará a separação desses alarmes por categoria. Os que pertencerem às categorias A1 e A3 serão levados para o escalonador de candidatos (onde será efetuado o processamento para a indicação dos componentes suspeitos por provocarem os alarmes), enquanto os demais, alarmes de categoria A2, passarão por uma triagem no eliminador de redundância, cuja função é o descarte de alarmes redundantes e por fim os alarmes remanescentes serão encaminhados para o escalonador de candidatos.

No escalonador de candidatos será feita uma comparação entre os alarmes do domínio da rota física, os alarmes A2 relevantes, oriundos do eliminador de redundância e, se existirem, os alarmes A1 e A3 do selecionador de alarmes. No domínio da rota física poderão ser encontrados todos os elementos da rede e associados a cada um deles os respectivos domínios de alarmes. Para cada elemento de rede pertencente a um canal, existe um conjunto de componentes de rede que enviarão alarmes se este elemento vir a falhar, o conjunto formado pelos componentes que alarmarão é chamado de domínio de alarme (SOUSA *et al.*, 2005). Terminada essa comparação só restarão alarmes que contribuirão diretamente para a localização da falha, então uma análise inversa no domínio de alarmes é feita para encontrar o conjunto dos componentes suspeitos que serão entregues a gerência.

No conjunto de componentes suspeitos estão todos os componentes que, estando em condição anormal, causariam o envio de todos os alarmes que chegaram à gerência. Na Figura 32 está a representação gráfica do processo de localização de falhas.

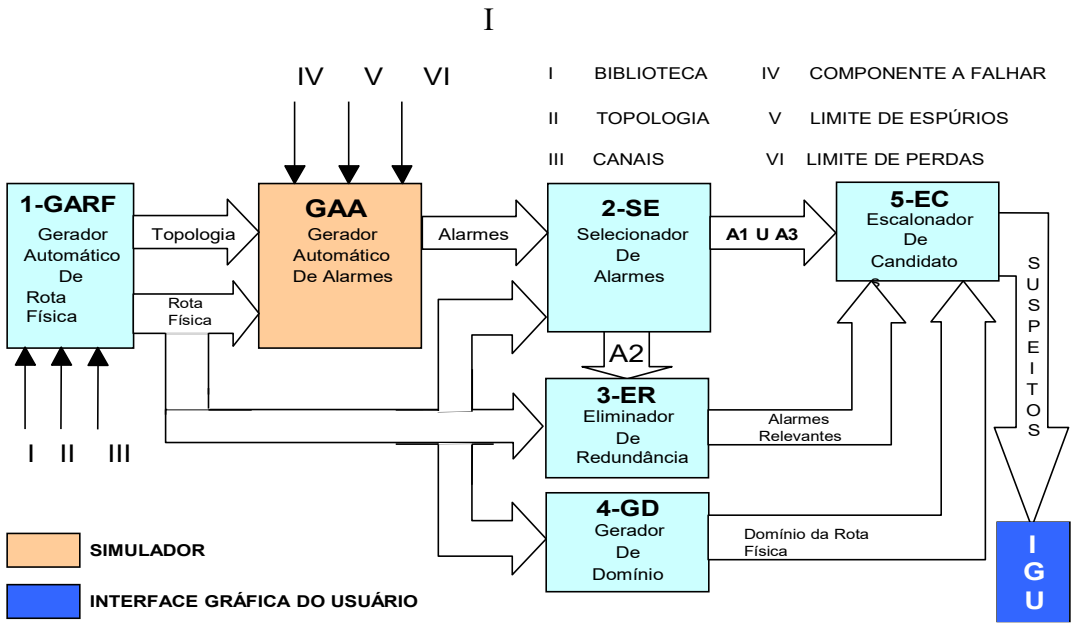


Figura 32. Processo de Localização de Falhas do ASP. Elaborada pelo autor.

4.2.1.1 *Gerador automático de rota física*

A partir das informações de arquivos XML é que se inicia o processo de preparação do sistema de localização de falhas. Os referidos arquivos XML são os seguintes: Biblioteca, Topologia e Canais. Ao final do processamento dos dados de entrada é gerada uma descrição detalhada dos canais ao nível de componentes de rede, isto é, os canais que eram somente definidos pelos nós que estão em comunicação agora passam a ser representados por todos os componentes de rede - componentes dos nós e fibras que estão sendo utilizados como caminho pelo sinal óptico. Na Figura 33 está a representação gráfica do gerador automático da rota física, GARF.

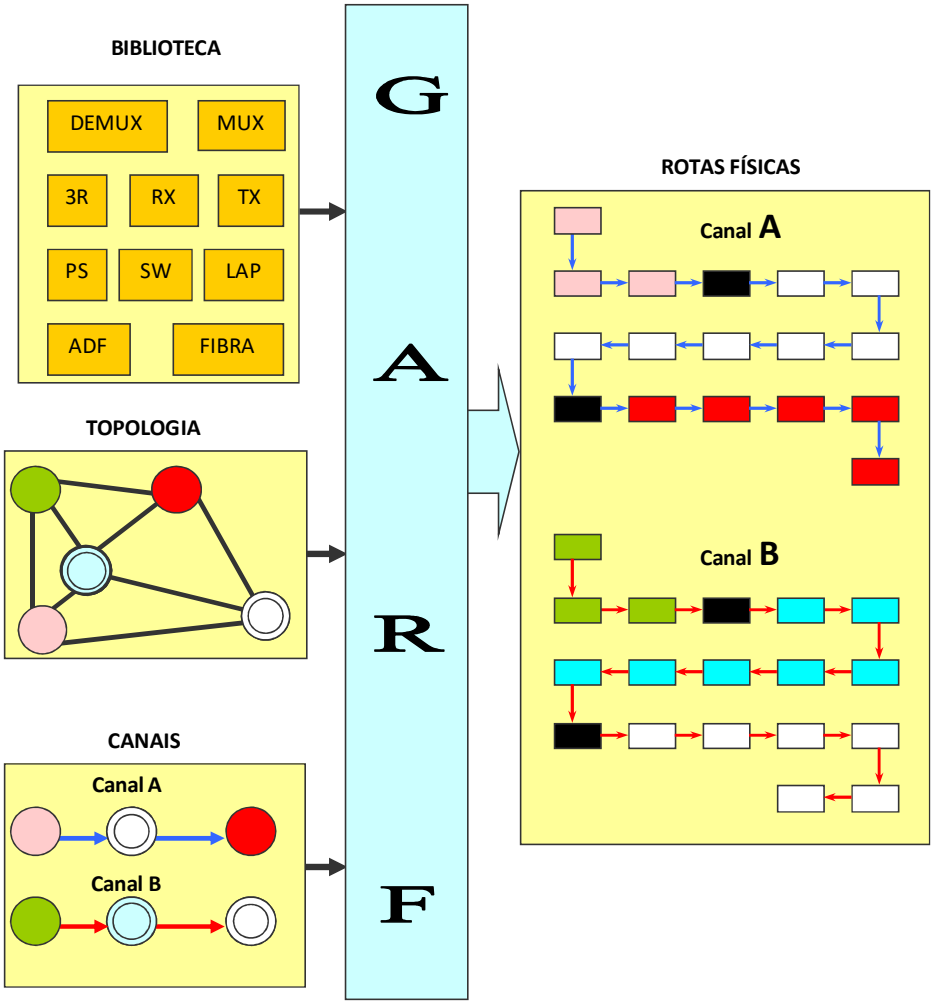


Figura 33. GARF - Gerador Automático de Rota Física. Elaborada pelo autor.

Rota física

A rota física é um conjunto de listas formadas pelos componentes de rede que estão sendo utilizados, isto é, representa todos os canais estabelecidos, componente a componente. Na entrada do GARF a informação sobre os canais é inserida da seguinte forma:

Inicialmente, deve-se abrir um editor de texto para XLM e, em seguida, o nome do canal e os nós que compõem o mesmo devem ser digitados, como pode ser observado na listagem em XML abaixo:

<?xml version="1.0" encoding="UTF-8" ?>

- <!--

edited with XML Spy v4.2 U (http://www.xmlspy.com) by Aminadabe (Aminadabe)
-->

</Canal>

<Canal id="c5" nome="Canal #5">

<Elementos idElemento="n08" />

<Elementos idElemento="n10" />

<Elementos idElemento="n15" />

</Canal>

A listagem acima representa a inserção do canal 5 via XML no GARF. Este é formado pelos nós 8, 10 e 5. O canal 5 inicia no nó 8, passa pelo nó 10 e termina no nó 15. Essas serão as informações que serão inseridas no GARF.

Na saída do GARF após a análise das informações inseridas pelos arquivos XML (Biblioteca, Topologia e Canais), os canais são apresentados em uma forma mais detalhada, componente a componente, que é a rota física. Por exemplo, a rota física do Canal 5 é apresentada na listagem em XML abaixo:

</canal>

<canal id="c5" nome="Canal 5">

<componente id="8/tc_lap/:0 8 0 0:" nome="No 8/LAP" />

<componente id="8/tc_sw/:1 8 0 1:" nome="No 8/SW" selfalarm="1" />

<componente id="8/tc_tx/:3 8 0 15:" nome="No 8/TX" selfalarm="1" maskalarm="1" />

<componente id="8/tc_mux/:0 8 1 0:" nome="No 8/Mux" />

<componente id="tc_fb/:0 0 8 10:" nome="Fibra" />

<componente id="10/tc_adf/:1 10 0 1:" nome="No 10/ADF" selfalarm="1" />

<componente id="tc_fb/:0 0 10 15:" nome="Fibra" />

<componente id="15/tc_dmx/:0 15 0 10:" nome="No 15/Demux" />

<componente id="15/tc_ps/:2 15 15 1:" nome="No 15/PS" outalarm="1" />

<componente id="15/tc_rx/:2 15 15 2:" nome="No 15/RX" outalarm="1" />

<componente id="15/tc_3r/:2 15 15 3:" nome="No 15/3R" outalarm="1" />

<componente id="15/tc_sw/:1 15 0 1:" nome="No 15/SW" selfalarm="1" />

<componente id="15/tc_lap/:0 15 0 0:" nome="No 15/LAP" />

</canal>

Como pode ser observado acima, a representação do canal 5, após passar pelo GARF, passou a ser mais detalhada. Além da indicação dos nós por onde é transmitido o sinal óptico tem-se a informação por quais elementos, fibra e componentes dos nós, está passando o sinal óptico, assim como as características desses elementos. As informações que foram adicionadas são provenientes do processamento dos dados da Biblioteca.

4.2.1.2 *Simulador - Gerador automático de alarmes*

O Gerador Automático de Alarmes, GAA, será usado para gerar sequências de alarmes, conforme alguns critérios. Os dados de entrada do simulador estão divididos em dois tipos: ajustáveis e variáveis.

a. Os ajustáveis ou de inicialização - são aqueles que são inicializados de acordo com a configuração inicial do ambiente a ser simulado, eles são os seguintes: topologia e a rota física;
b. Os variáveis - são os que são modificados após a inserção dos dados ajustáveis, pois são aqueles destinados a informar quais são os elementos que deverão falhar e qual a quantidade de alarmes falsos e/ou perdidos. Conforme a topologia e a rota física informadas, anteriormente. Os alarmes falsos e perdidos são inseridos para se fazer uma análise da robustez do algoritmo.

O GAA proverá na saída um conjunto de alarmes de acordo com os dados fornecidos, isto é, emitirá na saída um conjunto de alarmes, $\boldsymbol{A}$, correspondente a uma falha no elemento que foi escolhido na entrada. O GAA, para gerar o conjunto de alarmes $\boldsymbol{A}$, obedece todas as

características da rede – limitações impostas pela Biblioteca, Topologia e Canais. O conjunto de alarmes ***A*** poderá ter o número de elementos alterado de acordo com os valores das entradas de: Limites de Espúrios e Limites de Perdas. Na entrada de Limites de Espúrios, que pode ser manual ou automática, é definida a quantidade de alarmes que devem ser adicionados ao conjunto de alarmes ***A***. A entrada de Limites de Perdas trabalha da mesma maneira que a entrada de Limites de Espúrios, mas ao invés de alarmes falsos é definido a quantidade de alarmes pertencentes ao conjunto de alarmes ***A*** que deverão ser extraídos.

Quando for definido para o simulador qual componente deve falhar, este indicará qual ou quais alarmes devem ser emitidos para a gerência. Vale ressaltar que o algoritmo do simulador funciona independente do ASP. A geração de alarmes pelo GAA ocorre da seguinte maneira: quando um componente é escolhido para falhar o GAA verifica qual a categoria desse componente e dos demais que estão à frente dele dentro do canal até chegar em um transmissor. Caso existam componentes de categoria A1, A2 e/ou A3 o GAA gerará alarmes referentes a esses componentes.

4.2.1.3 *Selecionador de alarmes*

No Selecionador de Alarmes é verificado, inicialmente, se os alarmes recebidos foram gerados por componentes de rede que façam parte de algum canal do conjunto das rotas físicas, **RF**, que é composto por todos os canais estabelecidos na rede. Caso existam alarmes que não pertençam a **RF**, os mesmos serão descartados e os alarmes restantes serão alocados em dois grupos distintos. Um grupo será formado pelos alarmes gerados por componentes de rede da categoria A2 e o outro será formado pelos alarmes emitidos por componentes das categorias A1 e A3. O primeiro grupo formará o conjunto dos alarmes dos componentes não suspeitos, (ACNS), e o segundo, o conjunto dos alarmes dos componentes suspeitos 1, (ACS1). Resumidamente, um alarme ***a*** pertencerá ao conjunto ***A*** e será um elemento do conjunto ACNS, se e somente se o componente que enviou o alarme ***a*** (***a.fonte***) pertencer ao conjunto dos componentes de rede (***CR***) tal que exista ***a.fonte*** pertencente a algum canal ***K***, com ***K*** pertencente ao conjunto das rotas físicas (***RF***) e ***a.fonte*** pertencente aos conjuntos dos alarmantes externos (***A2***). Matematicamente, o conjunto dos alarmes dos componentes não suspeitos pode ser representado pela Expressão 1 (SOUSA *et al.*, 2005):

$$ACNS = \left\{ \begin{array}{l} a \in A \Leftrightarrow a.fonte \in CR \mid \exists\, a.fonte \in K, \\ com \quad K \in RF \wedge a.fonte \in A2 \end{array} \right\} \qquad (1)$$

De forma simplificada, o ACS1 é composto por componentes ***c*** que pertencem ao ***CR***, tal que o canal ***K*** pertença a ***RF*** com a posição de ***c*** dentro do canal ***K*** diferente de zero e, além disso, exista um alarme ***a*** pertencente a ***A*** com o componente ***c*** igual ao componente que enviou o alarme ***a*** (***a.fonte***) e ***a.fonte*** pertencente ao conjunto dos elementos ***A1*** ou ***A3***. Matematicamente, o conjunto dos componentes suspeitos 1 pode ser representado pela Expressão 2 (SOUSA *et al.*, 2005):

$$ACS\ 1 = \left\{ \begin{array}{l} c \in CR \mid K \in RF \ \ com \ \ Loc\ (c, K) \neq 0 \wedge \exists\ a \in A \ com \\ c = a.fonte \ \ \wedge \ \ a.fonte \ \in A1 \bigcup A3 \end{array} \right\} \tag{2}$$

Na Figura 34 está a representação gráfica do selecionador de alarmes, SA:

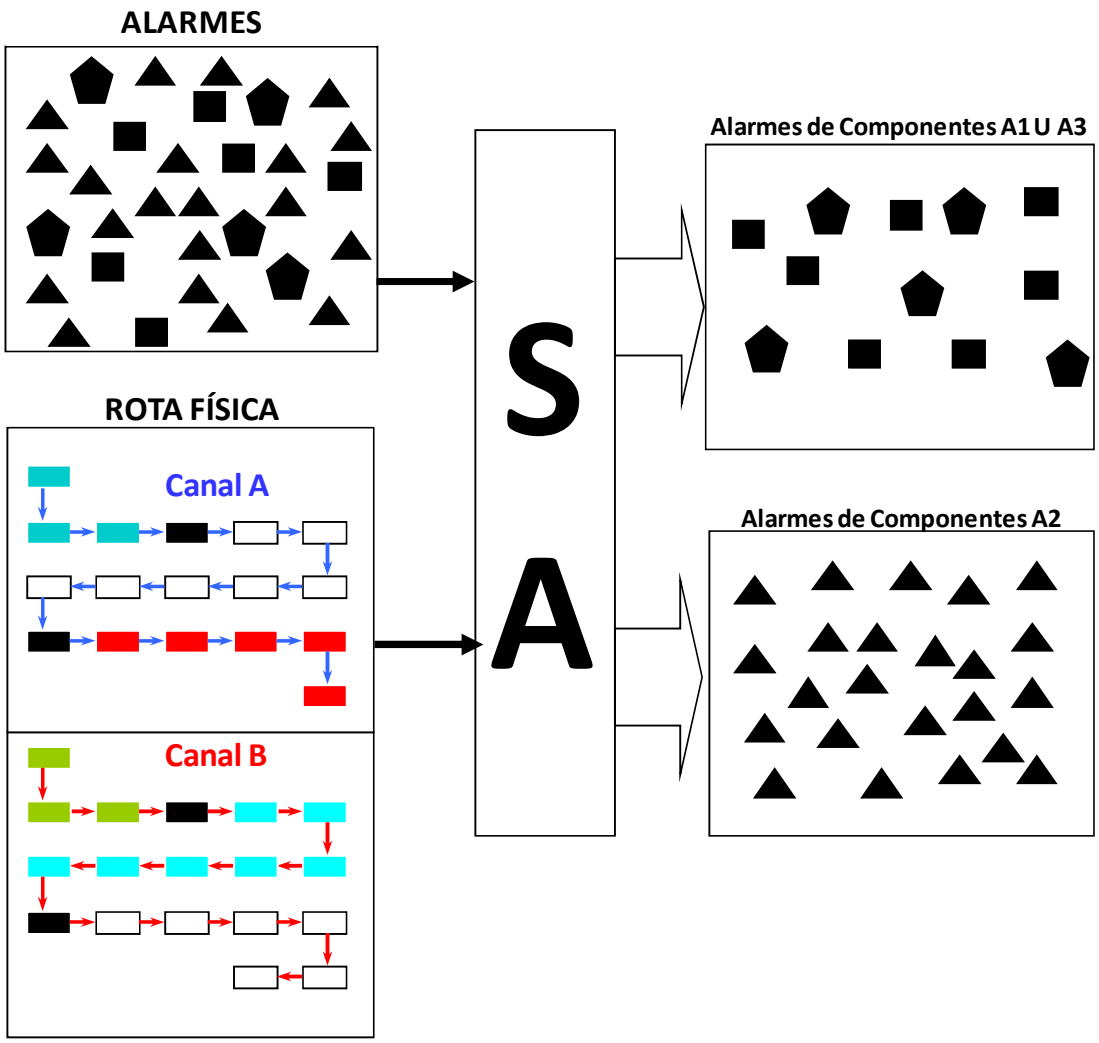


Figura 34. SA - Selecionador de Alarmes. Elaborada pelo autor.

4.2.1.4 Eliminador de redundâncias

Neste módulo os ACNS irão passar por uma filtragem para a eliminação de alarmes que não trarão nenhum ganho para a localização dos componentes falhos. Para que isso ocorra, o Eliminador de Redundância utilizará as informações da rota física, que advém do GARF. De posse da rota física o eliminador de redundância terá as informações das posições dos componentes dentro do canal, o que é primordial para o processo de triagem dos alarmes pertencentes ao ACNS. Admitindo que é menos provável ter-se x+1 falhas do que x falhas, então alguns dos alarmes do conjunto ***A*** serão descartados. Assumindo que Loc (c,K) significa localização do componente c dentro do canal K. Então, considerando Loc (ci, K) +1 = Loc (ci+1, K), e que ci e ci+1 são componentes de rede de categoria A2, então na ocorrência de algum evento em um componente de rede c, onde c ∈ K, se c estiver localizado antes de ci, isto é Loc (c,K) < Loc (ci,K) e não existir nenhum componente de categoria A3 entre c e ci, o alarme emitido pelo componente ci+1 poderá ser desconsiderado, pois ele não trará nenhum ganho para a localização da(s) falha(s). Quando não existir nenhum componente A3 entre ci e ci+1 (no caso em que os dois estão disjuntos) pode-se utilizar o mesmo princípio e efetuar a exclusão do alarme emitido por ci+1. O resultado obtido na saída do eliminador de redundância será um conjunto composto somente por alarmes com informações relevantes para a localização dos componentes falhos, este conjunto é denominado de alarmes relevantes, ***AR***. De maneira resumida, um alarme a_n pertencerá a ***ACNS*** e fará parte de ***AR***, se e somente se a_n pertencer ao conjunto ***A2*** tal que o componente que enviou a_n (a_n***.fonte***) pertença a algum canal ***K,*** com ***K*** pertencendo a ***RF***. E, além disso, para todo e qualquer a_{n-1}***.fonte*** pertencente a ***ACNS,*** tivermos um trecho do canal onde não há componentes de categoria A3 (β - caminho passivo) entre a_{n-1}***.fonte*** e a_n***.fonte***. A representação matemática é dada pela Expressão 3 (SOUSA *et al*, 2005):

$$AR = \left\{ \begin{array}{l} a_n \in ACNS \Leftrightarrow a_n \in A2 \mid \exists\, a_n.fonte \in K \ com \\ K \in RF \wedge \forall\, a_{n-1}.fonte \in ACNS\ ,\ a_{n-1}.fonte \times \beta \times a_n.fonte \end{array} \right\} \quad (3)$$

Na Figura 35 está a representação gráfica do eliminador de redundância, ER:

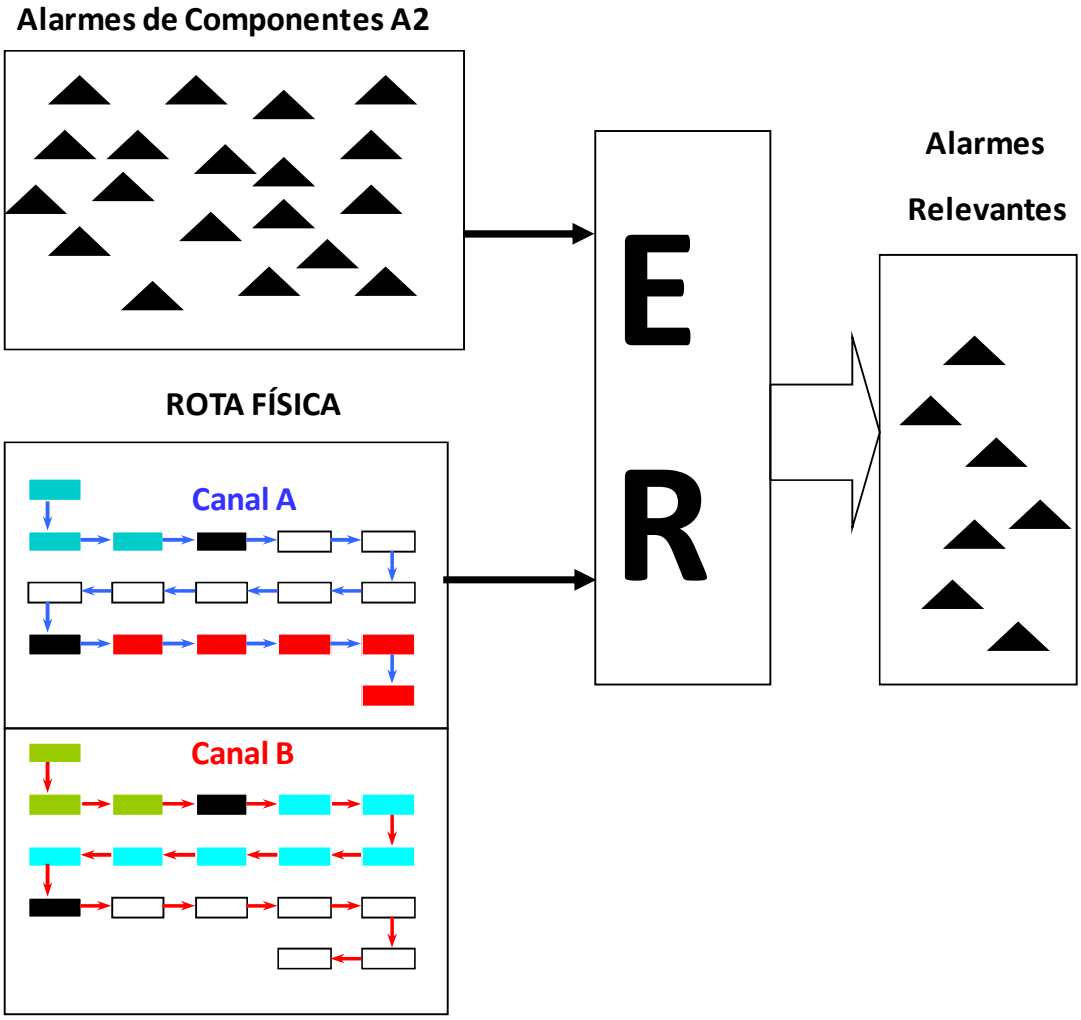


Figura 35. ER – Eliminador de Redundância. Elaborada pelo autor.

4.2.1.5 *Gerador de domínio*

Neste módulo encontra-se a base do algoritmo de localização de falhas do modelo *ASP*, pois ele é responsável pela geração do domínio de alarmes de todos os componentes da rede, que estão em comunicação. Para ser possível a geração do domínio de alarmes o gerador necessita como dado de entrada a rota física, que é entregue pelo GARF. O gerador de domínio é o responsável por calcular para cada elemento da rede pertencente à rota física, o conjunto de elementos que enviarão alarmes se cada elemento vier a falhar. Poderão ser emitidos para a gerência diferentes tipos e quantidades de alarmes. Essa variação dependerá fundamentalmente

de dois fatores: da posição em que o componente está no canal e da quantidade de canais que estão passando por ele.

Na Figura 36 está a representação gráfica do gerador de Domínio, GD:

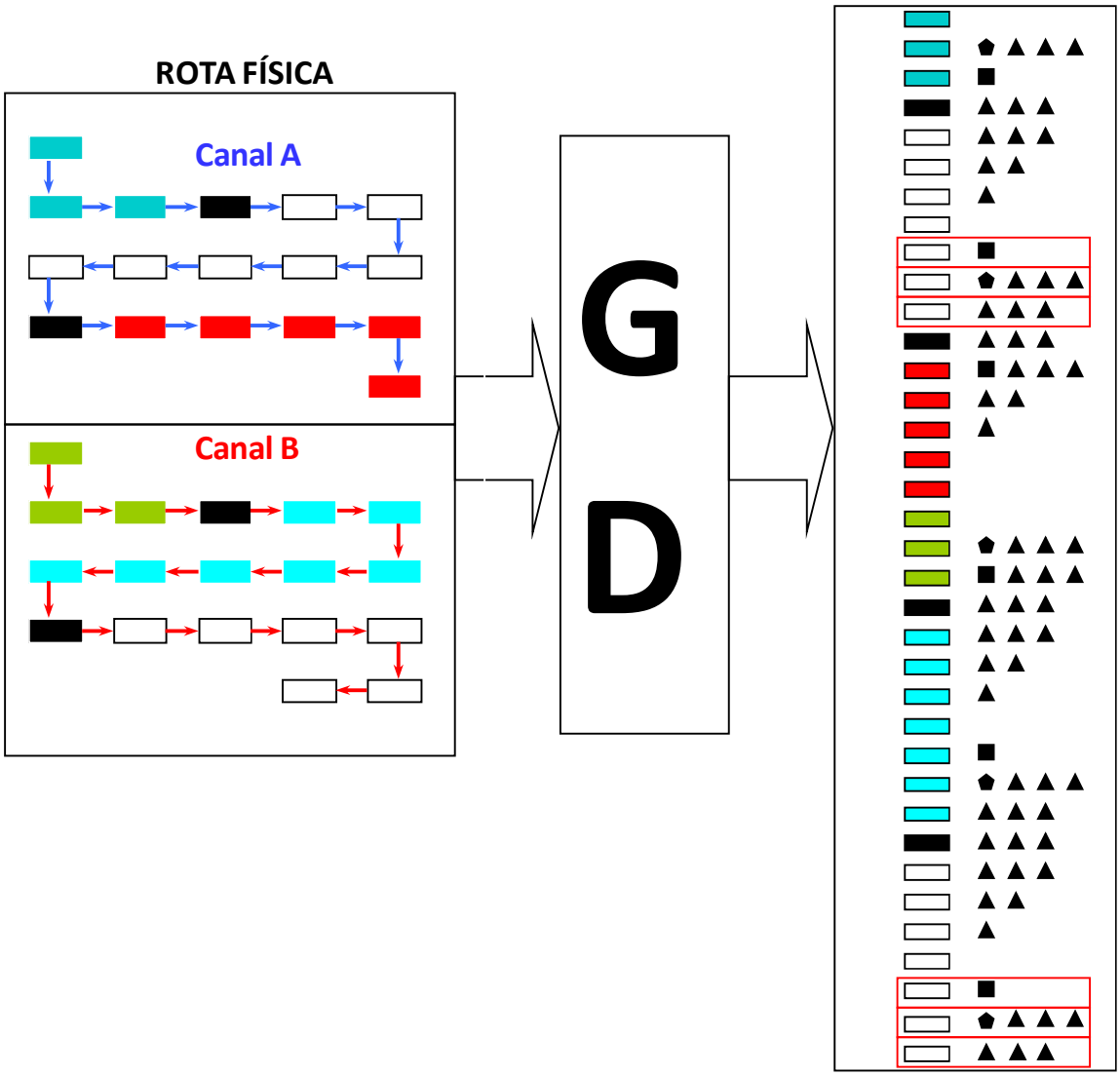


Figura 36. GD – Gerador de Domínio. Elaborada pelo autor.

4.2.1.6 *Regras do domínio de alarmes*

O domínio de alarmes está divido em três grupos: os dos elementos iniciais, os de passagem e os finais. O fator determinante que indica em qual grupo de elementos um

componente de rede irá fazer parte será a posição do nó ao qual ele pertence dentro do canal. Os elementos de rede que farão parte do grupo dos elementos iniciais serão aqueles por onde flui o sinal óptico e que pertencem aos nós que ficam no início do canal. Por sua vez, os elementos que farão parte do grupo dos elementos finais serão aqueles por onde flui o sinal óptico e que pertencem aos nós que ficam no fim do canal. Por conseguinte, os elementos de rede que pertencerem ao restante dos nós do canal e por onde flui o sinal óptico, que não ficam nem no início e nem no final do canal, farão parte do grupo dos elementos de passagem.

Na Figura 37 está indicado o significado dos símbolos utilizados pelos gráficos dos Domínios de Alarmes dos componentes de rede diante de uma falha ou evento.

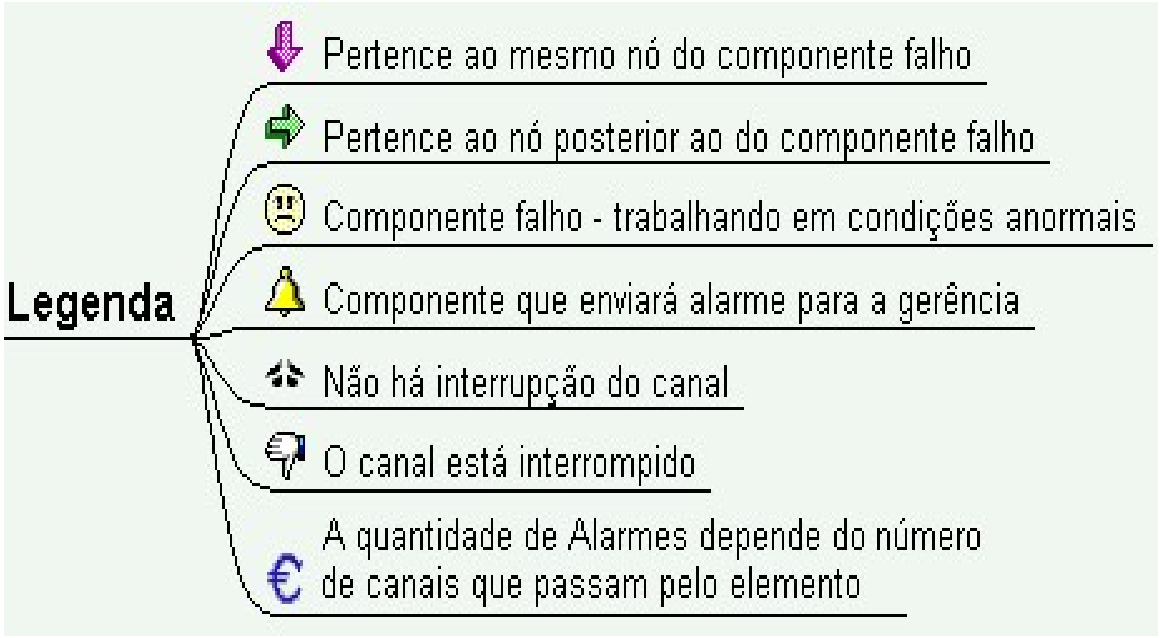


Figura 37 – Legenda dos sinais de comportamento dos componentes de rede. Elaborada pelo autor.

A representação gráfica do domínio de alarmes dos elementos iniciais, componentes dos nós locais e centrais que estão em operação nesta configuração, de um canal é mostrada na Figura 38.

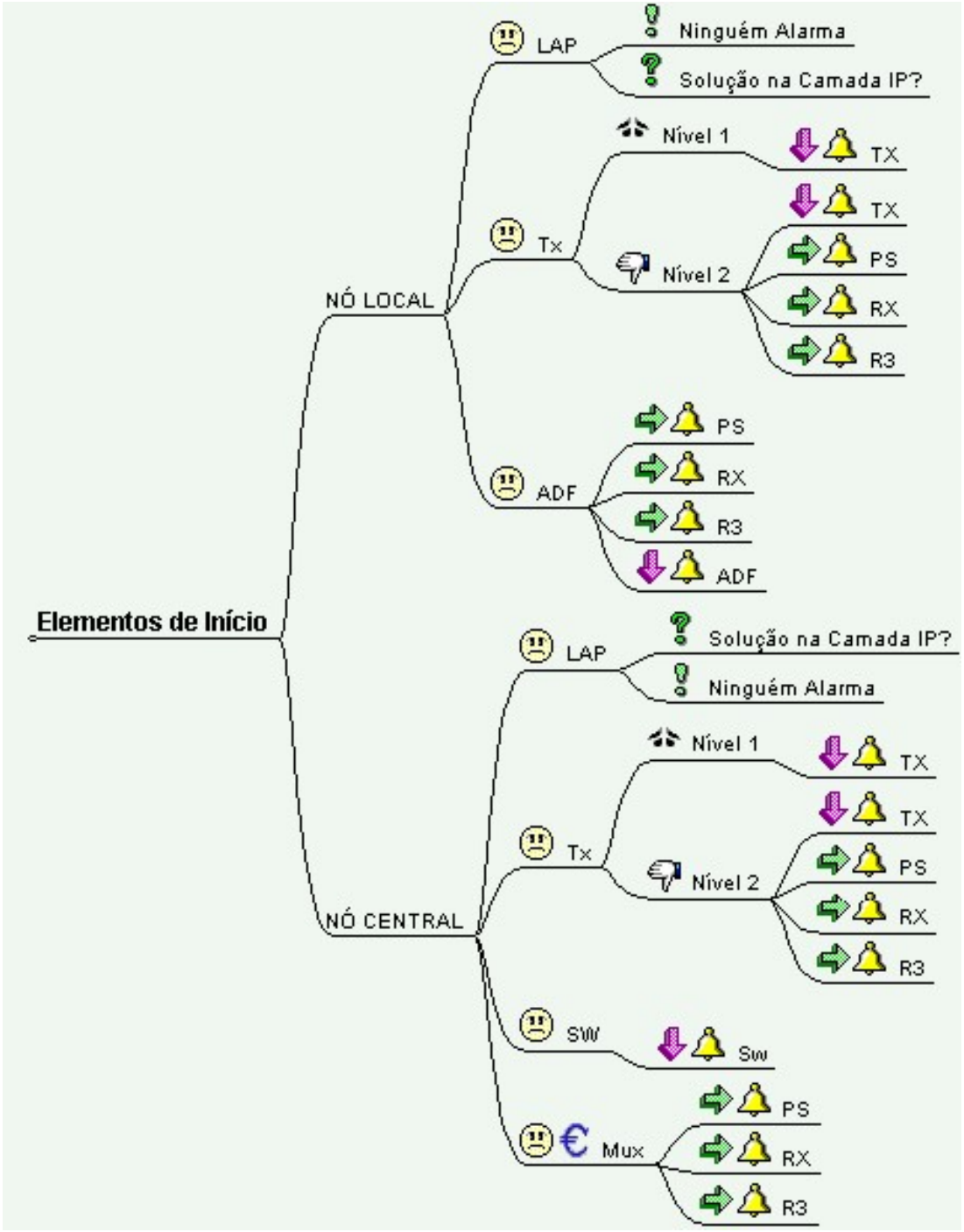


Figura 38. Domínio de alarmes dos elementos iniciais de um canal. Elaborada pelo autor.

O domínio de alarmes dos elementos de passagem (fibras e componentes dos nós locais e centrais que estão em operação nesta configuração) de um canal é mostrado na Figura 39.

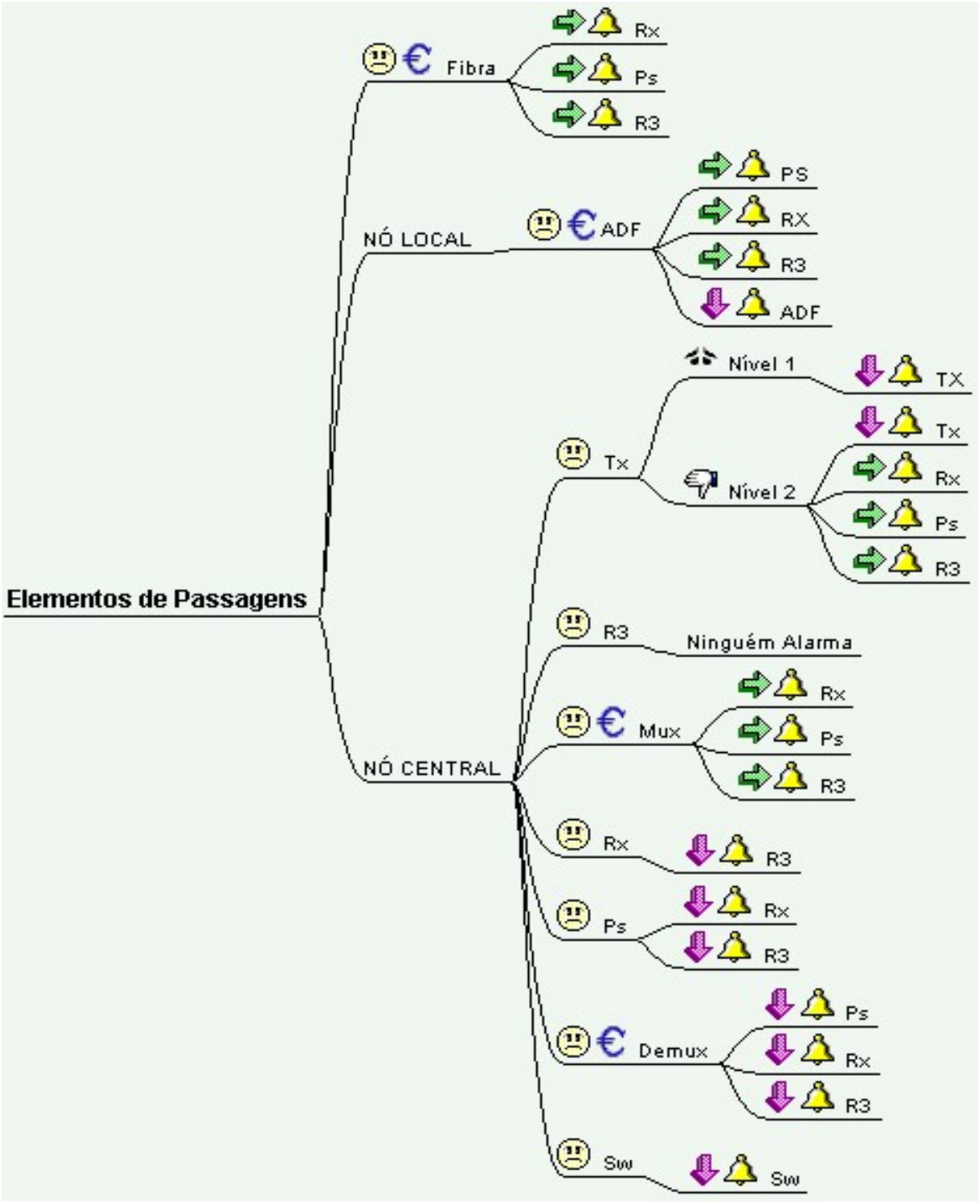


Figura 39. Domínio de alarmes dos elementos passagem de um canal. Elaborada pelo autor.

Na Figura 40 pode-se observar o domínio de alarmes dos elementos finais (componentes dos nós locais e centrais que estão em operação nesta configuração) de um canal.

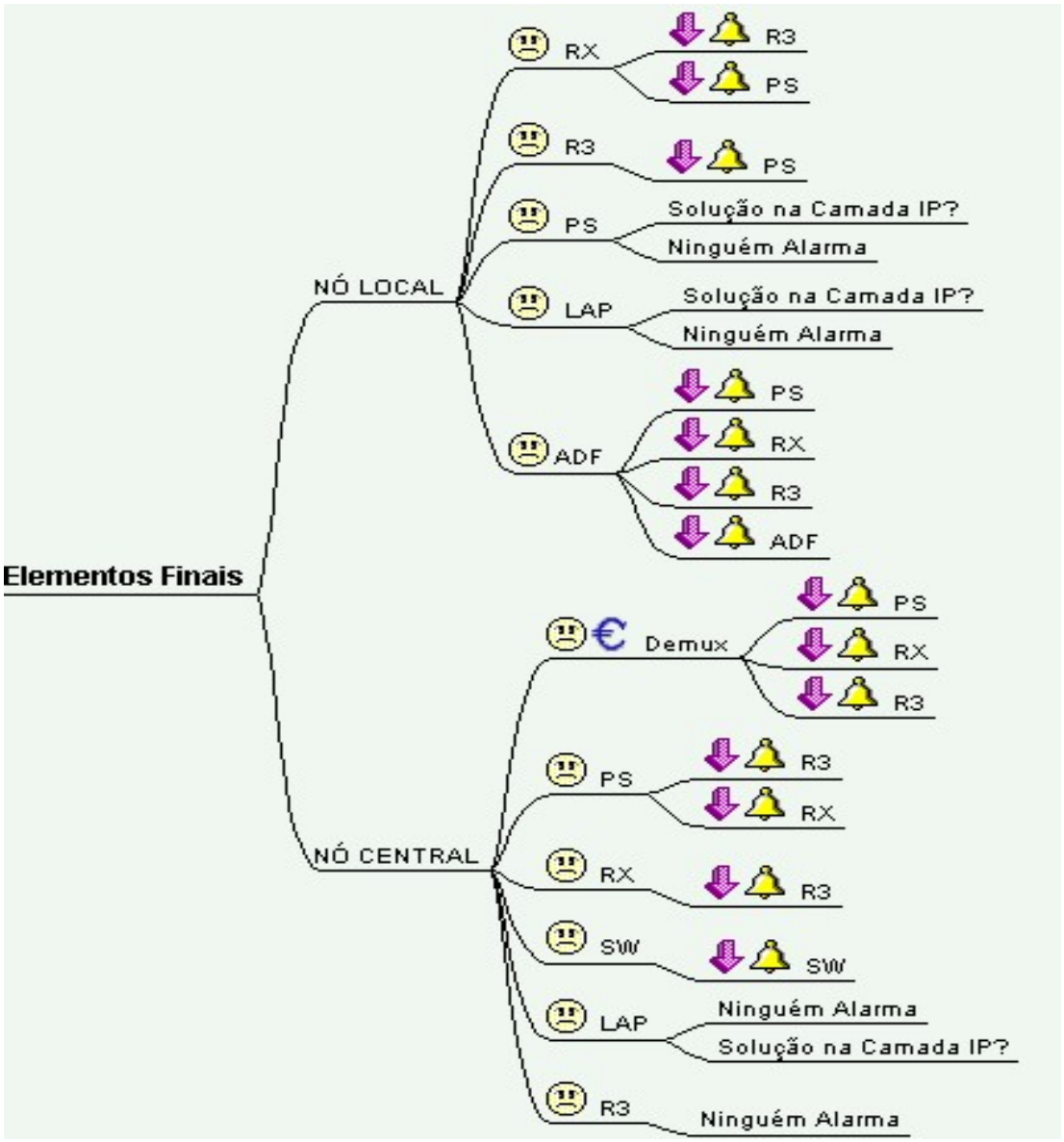


Figura 40. Domínio de alarmes dos elementos finais de um canal. Elaborada pelo autor.

4.2.1.7 *Escalonador de candidatos*

De posse dos alarmes A1 e A3, caso estes existam advindos do selecionador de alarmes, dos alarmes A2 relevantes e do domínio da rota física, o escalonador de candidatos processará todas estas informações e apresentará para a interface gráfica do usuário, IGU, o conjunto dos candidatos suspeitos.

Os prováveis candidatos são todos os componentes de rede que, individualmente ou em conjunto, são os responsáveis por causar os alarmes que foram gerados na rede e enviados para a gerência.

Na etapa inicial do escalonamento de candidatos o conjunto ACS1 (alarmes de componentes suspeitos 1), que advém dos componentes A1 e A3 vão dar origem ao conjunto dos componentes suspeitos 1 (CS1), que ficarão aguardando pela geração do conjunto dos componentes suspeitos 2 (CS2). Este último resultará da comparação entre o conjunto dos alarmes relevantes e o domínio de alarmes da rota física, (DARF). Os alarmes coincidentes entre os dois indicarão os possíveis componentes falhos, que causaram todos os alarmes ou parte deles, pois encontrando no DARF o domínio de alarmes equivalente aos alarmes relevantes, basta associar aos componentes que possuem aqueles domínios de alarmes.

Se um alarme ***a*** é emitido por um componente de rede de categoria A2 e há um caminho passivo β com ***c***, sendo que ***c*** é um componente de rede que pode ter causado o alarme ***a***, então pode-se dizer que ***c*** é um componente falho (SOUSA *et al.*, 2005). O resultado desta comparação gerará o conjunto componentes suspeitos 2, CS2, que poderá ser composto por componentes falhos de diferentes categorias P, A1, A2 e A3. De forma simplificada, o ***CS2*** será composto por componentes ***c*** que pertençam ao conjunto ***RF***, se e somente se ***c*** pertencer ao ***CR***, tal que o canal ***K*** pertença a ***RF*** com a posição de ***c*** dentro do canal ***K*** diferente de zero e, além disso, exista um alarme ***a*** pertencente ao ***DARF*** ou ao conjunto ***AR*** com um caminho passivo β entre o componente ***c*** e o componente que enviou o alarme ***a*** (***a.fonte***). Matematicamente, o conjunto dos componentes suspeitos 2 pode ser representado pela Expressão 4 (SOUSA *et al.*, 2005):

$$CS2 = \left\{ \begin{array}{l} c \in RF \Leftrightarrow c \in CR \mid \exists\ K \in RF\, com \\ Loc(c,K) \neq 0\ \wedge\ \exists\ a \in DARF \bigcup \qquad com \\ c \times \beta \times a.fonte = 1 \end{array} \right\} \tag{4}$$

De maneira resumida, o ***DARF*** será composto por componentes ***c*** que pertencem a ***A1*** ou ***A2*** ou a ***A3***, se e somente se o canal pertencer a ***RF*** com a posição de dentro do canal ***K*** igual ou maior do que a primeira posição e, além disso, para todo e qualquer componente pertencente a ***CR*** tenha-se c_j, c_i e ***c*** em ***K*** com c_j a frente de c_i e ***c*** a frente de c_j, com c_j não pertencendo a categoria ***A3***.A representação matemática do ***DARF*** pode ser vista na Expressão 5 (SOUSA *et al.*, 2005):

$$DARF(c_i) = \left\{ \begin{array}{l} c \in A1 \bigcup A2 \bigcup A3 \Leftrightarrow K \in RF, \\ 1 \leq Loc(c_i,K)\ \wedge\ \forall c_j \in CR \\ com \quad Loc(c_i,K) \leq Loc(c_j,K) \leq Loc(c,K), c_j \notin A3 \end{array} \right\} \tag{5}$$

A união dos componentes advindos dos conjuntos CS1 e CS2 formarão o conjunto dos suspeitos, S. Caso haja componentes repetidos, esses serão descartados e o restante dos componentes será apresentado ao operador da rede. A duplicidade de componentes em CS1 e CS2 pode vir a ocorrer devido à falha em componentes de categorias A1 ou A3, pois ocorrerá envio de alarmes por parte deles, por serem alarmantes internos, assim como pelos componentes A2 que se encontrarem à frente e no mesmo canal que eles. Resumidamente, o conjunto ***PS*** será formado por componentes ***c*** pertencentes ao conjunto ***RF***, se e somente se ***c*** pertencer ao ***CR***, tal que exista um alarme ***a*** pertencente a ***A*** com o componente ***c*** igual ao componente que enviou o alarme ***a*** (***a.fonte***). Matematicamente, o conjunto dos suspeitos ***PS*** pode ser expresso pela Expressão 6 (SOUSA *et al.*, 2005):

$$PS = \left\{ c \in RF \Leftrightarrow c \in CR \mid \exists\, a \in A, com \quad a.fonte = c \right\} \tag{6}$$

Esta é uma base teórica para o tratamento de risco proposto no modelo. O modelo ASP foi implementado em uma ferramenta de *software* chamada *ASP software* (Figura 41).

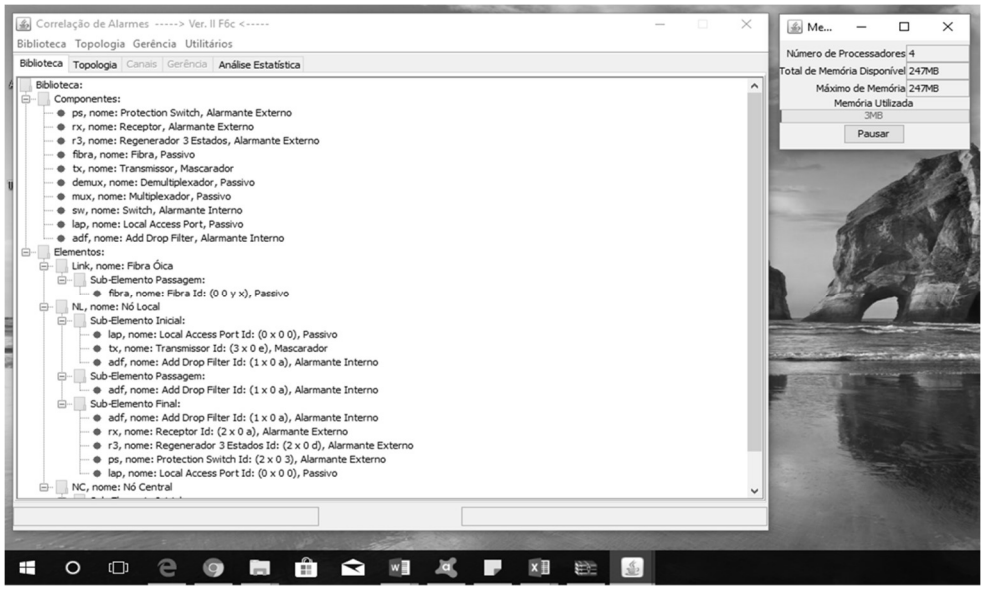


Figura 41. Interface do software *ASP.* Elaborada pelo autor através do ASP.

4.2.2 Utilização do modelo ASP

Conforme mostrado na Figura 40, para utilização do modelo ASP, os gestores devem executar os seguintes passos:

PASSO 1 - Modelagem da topologia da rede óptica no ASP. As informações referentes à topologia, canais e elementos da rede óptica a serem avaliados são informados através da interface de entrada do *software ASP,* o qual automatiza o modelo proposto nesta tese.

PASSO 2 - Definição dos parâmetros de avaliação do negócio no modelo. Os seguintes parâmetros são informados como entrada no modelo proposto:

- Grau de abrangência do modelo: para a realização das simulações, o modelo permite a escolha da abrangência do cálculo de risco, onde a estimativa do impacto pode ser realizada por categoria de elementos de rede ou por cada elemento de rede da topologia da rede avaliada.
- Definição da fórmula de cálculo do impacto de um elemento de rede para o negócio: A realização da avaliação de impacto (B.I.A.) para falhas de redes é um processo muito complexo porque existe uma dependência enorme de outros serviços em função do serviço de rede. Dependendo do tipo de negócio de cada organização, o impacto de um

elemento pode ser maior ou menor. O modelo proposto é simples e flexível, permitindo a definição e utilização de diversas fórmulas (propostas) para o cálculo do impacto de um elemento de rede para o negócio. Nos cenários de simulação vinculados ao estudo de caso apresentado neste trabalho foram propostas e utilizadas duas fórmulas de cálculo simplificadas, validadas pelos gestores e fundamentadas no objetivo de negócio manter o serviço de rede com alta disponibilidade. Cada fórmula é apresentada na sequência.

PASSO 3 - Definição dos parâmetros de calibragem do modelo

O modelo ASP utiliza uma abordagem baseada no consenso entre os gestores, para a estimativa dos parâmetros para sua utilização. A estratégia tem como base o método *Delphi*, contando com duas rodadas de avaliação, bem como com a utilização de questionários como ferramenta de coleta das informações dos gestores. A descrição de atividades das duas rodadas de avaliação é feita na sequência.

3.1. **Primeira rodada de avaliação:** os gestores estimam os seguintes parâmetros, através da resposta de questionários específicos. Para cada uma das respostas, o gestor deve apresentar a motivação (justificativa) utilizada na escolha realizada.

Para a rede óptica em geral:

- Quantidade de serviços de TI que são dependentes da rede óptica avaliada (número);
- Percepção do gestor sobre a importância de se ter uma alta disponibilidade de rede para o negócio (respostas com escala de Likert)
    - Muito alta(5) - Alta(4) - Média(3) - Baixa(2) - Muito baixa (1).
- Percepção da importância para o negócio de se manter uma alta qualidade de serviços
    - Muito alta(5) - Alta(4) - Média(3) - Baixa(2) - Muito baixa (1).

Para cada categoria de elemento da rede óptica (topologia) ou para cada elemento de rede da topologia avaliada:

- Probabilidade de falha - percentual (0 - 100%)
- Impacto do reparo - percentual (0 - 100%) = (tempo médio de reparo / tempo médio entre falhas)
    - Tempo médio de reparo (dados estatísticos ou estimativa)
    - Tempo médio entre falhas (dados estatísticos ou estimativa)

- Relevância do elemento de rede para o negócio (pesos com base na escala de *Likert*)
    - Muito alta(5) - Alta(4) - Média(3) - Baixa(2) - Muito baixa (1).
    - Os critérios empíricos a serem considerados na escolha da relevância do elemento de rede para o negócio (também elicitados com os gestores) são:
        - Quantidade de serviços de TI dependentes da rede óptica
        - Importância da disponibilidade da rede óptica para o negócio
        - Importância da qualidade de serviço da rede óptica para o negócio
        - Importância do elemento de rede na topologia
        - Redundâncias existentes na topologia

As justificativas para as respostas dadas podem ser baseadas em respostas empíricas ou em dados estatísticos do negócio.

3.2. **Segunda rodada de avaliação:** São apresentados os resultados da primeira rodada de avaliação, bem como uma lista das respostas dos avaliadores e suas justificativas. Na etapa de escolha, os gestores estimam os mesmos parâmetros, através da resposta dos questionários específicos. Caso sejam convencidos por alguma das justificativas apresentadas, os gestores podem mudar suas respostas. Dessa forma, busca-se um consenso entre o grupo de avaliadores. Na segunda avaliação os gestores não necessitam apresentar justificativas sobre suas escolhas. Os resultados são tabulados e utilizados como entrada nas simulações do software que implementa o modelo *ASP*.

PASSO 4 - Execução da simulação do cenário através do modelo *ASP* (automatizado através da ferramenta de *software ASP*). O ambiente de simulação é configurado para gerar o domínio da rota física a partir da biblioteca, topologia, canais e alarmes (dados de entrada). No domínio da rota física, todos os componentes de rede que compõem qualquer canal são numerados e associados a cada um desses componentes e seus respectivos alarmes, que serão enviados aos gerentes se eles falharem. A próxima ação é verificar a existência de alarmes provenientes dos componentes A1 e A3. Os respectivos componentes são suspeitos potenciais se houver alarmes, sendo então adicionados na lista de componentes suspeitos. Ao verificar os alarmes provenientes dos componentes A2 de cada canal, o algoritmo leva apenas o primeiro componente alarmado de cada canal, caso existam. Essa estratégia elimina alarmes redundantes. O canal é analisado no caminho inverso, até chegar ao primeiro transmissor, para considerar o resto dos componentes A2. Este processo deve ser realizado em todos os canais. Na sequência, é gerada uma lista com todos os componentes alarmados A2 e o primeiro

transmissor. A lista gerada é usada para formar conjuntos, no sentido de verificar todos os componentes listados, um a um, verificando se eles são capazes de produzir os alarmes observados na função de gerenciamento, em caso de falha. Isso é feito comparando o domínio de alarme de cada componente com o domínio da rota física gerado no início do algoritmo. Os componentes que passaram no teste formam conjuntos diferentes. Quando nenhum componente passa no teste, o teste é realizado novamente usando pares de componentes e assim por diante. Os conjuntos formados são adicionados à lista de componentes suspeitos, após todas as análises de combinação. Na sequência, o modelo *ASP* estima o risco (*ERV*) para todos os elementos de rede que apresentaram alarmes na simulação. A Figura 31 mostrou o diagrama funcional do modelo *ASP,* enquanto a Figura 42 apresenta sua visão de utilização.

A estimativa de risco de um elemento de rede no modelo é feita através da fórmula *Valor esperado do risco* (VER_e) = *Probabilidade de falha* (P_e) x *Impacto* (i_e)

PASSO 5 - Análise dos resultados e priorização dos pontos críticos para medidas de redundância na rede óptica.

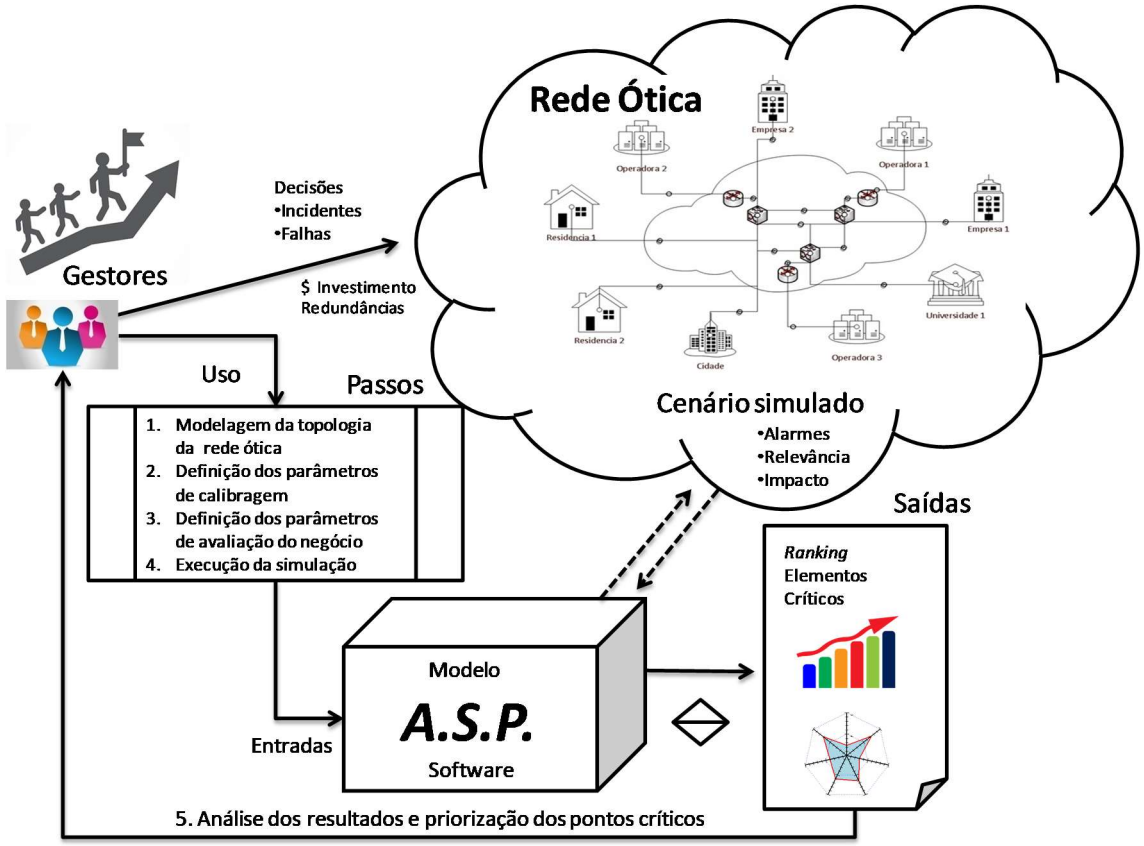


Figura 42. Visão de utilização do modelo ASP. Elaborada pelo autor.

4.2.2.1 *Cálculo do impacto do elemento de rede no modelo ASP*

O objeto da presente pesquisa está relacionado especificamente às redes ópticas. Foi observado que as redes ópticas geralmente são adotadas em *backbones*, na infraestrutura de provedores de serviços ou grandes empresas.

A análise de impacto de um elemento de rede está sujeita a aspectos do negócio, tais como a criticidade temporal dos seus serviços (por exemplo, algum serviço interrompido por falhas na infraestrutura óptica poderá ser concluído no futuro sem perda total de receita), tipo de acordo de nível de serviço (SLA) estabelecido e objetivo (SLO) afetado. Tais fatores influenciam e podem dificultar a análise do impacto nas medidas de negócio de interesse. Visando uma adaptação aos diversos cenários possíveis, como informado anteriormente, o modelo *ASP* é flexível, permitindo aos gestores a utilização de diferentes fórmulas para a estimativa do impacto de um elemento de rede.

Os gestores da empresa avaliada optaram pela busca e definição de formas de cálculo fundamentadas, simples, porém representativas, que possam ser utilizadas na estimativa do

impacto de um elemento de rede para o negócio. Durante o estudo de caso, foram propostas duas estratégias (fórmulas) para estimativa do impacto da falha de um elemento de rede óptica para o negócio, abrangendo as categorias de elementos de redes definidas no modelo *ASP*.

Foi considerada a dependência entre os elementos da rede e a topologia (influenciam a quantidade de alarmes gerada pelo modelo durante as simulações dos cenários). O grau de relevância do elemento de rede, utilizado nas duas propostas, é estimado pelos gestores. Na segunda fórmula proposta, os gestores consideraram que devido ao fato da importância do fator disponibilidade da rede para o negócio, poderia ser proposto o acréscimo do impacto do reparo (que influencia o cálculo da disponibilidade) na fórmula de estimativa do impacto da falha de um elemento de rede. As propostas utilizadas no estudo de caso realizado são mostradas na sequência.

Na primeira proposta para cálculo de impacto, utilizada nos cenários de 1 a 5 do estudo de caso realizado, o impacto do elemento de rede, ou seja, $i_e = \{1,2, \ldots E\}$ –em que E é o total dos elementos, é calculado (como mostrado nas equações 7, 8 e 9) pela média ponderada entre a relevância do elemento de rede (Ne_e) soma de alarmes de elemento (Ag_e) multiplicado pela relevância comercial (R_e - um peso), dividido pela relevância total dos alarmes (Ta_e), soma de todos os alarmes gerados multiplicados pela respectiva relevância (pesos). Formalmente:

$$i_e = \frac{Ne_e}{Ta_e} \qquad (7)$$

$$Ne_e = (Ag_e \times R_e) \qquad (8)$$

$$Ta_e = \sum_{1}^{E} (Ag_e \times R_e) \qquad (9)$$

Em que:

i_e - Impacto do elemento *e* na rede

Ag_e - Número de alarmes gerados quando o elemento *e* falha

R_e- relevância do elemento para o negócio (Muito alto - 5; Alto - 4; Médio - 3; Baixo - 2; Muito baixo - 1)

Ne_e - relevância do elemento de rede: relevância dos alarmes, é igual a soma dos alarmes do elemento, multiplicado pela relevância do elemento.

Ta_e - Relevância de alarmes totais: é igual a soma de cada alarme de elementos ativos, multiplicada pela relevância desses elementos.

Na segunda proposta para cálculo de impacto, utilizada em uma das duas simulações do quinto cenário do estudo de caso realizado, o impacto do elemento de rede, ou seja, i_e = {1,2, ... E} -E é o total dos elementos, é calculado (como mostrado nas equações 10, 11, 12 e 13) pela média ponderada entre a relevância do elemento de rede (Ne_e), soma de alarmes de elemento (Ag_e), multiplicado pela relevância comercial (R_e - um peso) e multiplicado pelo impacto do reparo do elemento e (ir_e), resultante da divisão entre o tempo médio de reparo do elemento e, dividido pelo tempo médio entre falhas do elemento e, dividido pela relevância total dos alarmes (Ta_e), soma de todos os alarmes gerados multiplicados pela respectiva relevância (pesos) e impacto do reparo dos elementos.

Formalmente:

$$i_e = \frac{Ne_e}{Ta_e} \qquad (10)$$

$$Ne_e = (Ag_e \times R_e \times ir_e) \qquad (11)$$

$$Ta_e = \sum_{1}^{E} (Ag_e \times R_e \times ir_e) \qquad (12)$$

$$ir_e = \frac{MTTR_e}{MTBF_e} \qquad (13)$$

Onde:

i_e - Impacto do elemento e na rede

ir_e - Impacto do reparo do elemento e na rede

Ag_e - Número de alarmes gerados quando o elemento e falha

R_e- relevância do elemento para o negócio (Muito alto - 5; Alto - 4; Médio - 3; Baixo - 2; Muito baixo - 1)

Ne_e - relevância do elemento de rede: relevância dos alarmes, gerado pela soma dos alarmes do elemento, multiplicado pela relevância do elemento.

Ta_e - Relevância de alarmes totais: gerada pela soma de todos os alarmes de elementos ativos, multiplicados pela relevância desses elementos.

$MTTR_e$ - tempo médio para reparo do elemento e.

$MTBF_e$ - tempo médio entre falhas do elemento e.

4.2.2.2 *Análise de risco*

A partir das entradas do processo proposto pelo modelo *ASP*, os gestores deverão realizar uma análise dos riscos identificados. Esta análise servirá para que o gestor tenha informações da probabilidade dos riscos ocorrerem e dos seus impactos. A Figura 43 ilustra o processo de análise dos riscos. A abordagem aqui apresentada tem fundamentação teórica na proposta de Nóbrega *et al*., (2014), adaptada para as atividades de análise de risco com o modelo *ASP*.

Como entrada para esse processo, tem-se a lista de riscos, gerada como saída do modelo *ASP*. A técnica utilizada nesse processo será a de análise de probabilidade e impacto, análise realizada em cima da probabilidade e do impacto de um determinado risco identificado (NÓBREGA *et al*., 2014). A categorização dos riscos identificará se o risco merece mais ou menos atenção por parte dos gestores. A análise de exposição dos riscos identificará o quanto a rede está exposta a riscos. Toda e qualquer informação importante do risco pode ser identificada na análise.

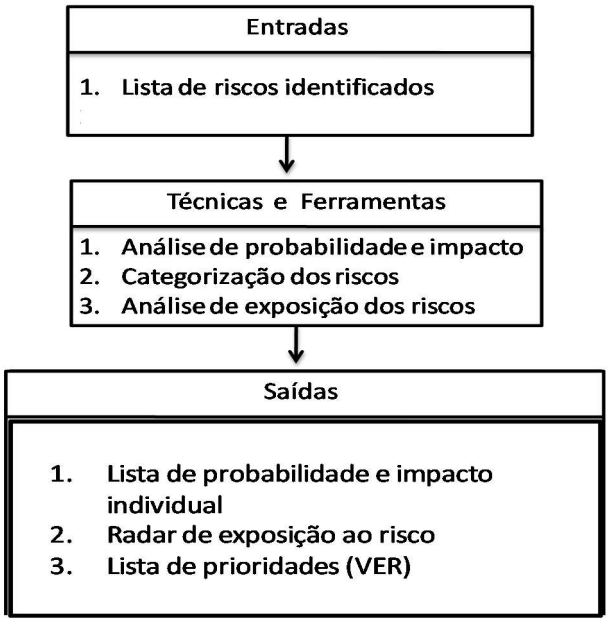


Figura 43. Análise de riscos a partir dos resultados do modelo ASP. Adaptado de Nóbrega *et al.*, (2014).

Deve ser utilizada uma lista com a probabilidade e o impacto individual de cada elemento de rede. Caso, necessário, pode ser utilizado um valor de sensibilidade para ajuste dos valores gerados e utilizados na lista (Ex. 30% de sensibilidade). O modelo *ASP* gera uma lista com o *ranking*, que pode ser interpretada da seguinte forma: quanto maior o valor esperado

(*VER*), maior a prioridade do risco. Após esta análise individual, o gerente poderá criar dois gráficos para demonstrar o estado da probabilidade e do impacto dos riscos analisados. Os gestores poderão categorizar os riscos a partir da utilização de cores (verde, amarelo e vermelho), de acordo com o grau de risco. Pode-se definir intervalos de valores para essas faixas, a critério dos gestores.

Descreve-se na sequência um método complementar que pode ser utilizado na análise de riscos, segundo Nóbrega *et al*., (2014). Devido a limitações de tempo, escopo e orçamento, essa proposta complementar apresentada nessa subseção foi avaliada e validada a nível conceitual junto aos gestores da empresa *Alpha*, devendo ser avaliada através de estudo de caso real em trabalhos futuros.

Os gestores devem executar uma análise simultânea dos riscos, analisando a probabilidade e o impacto do acontecimento de dois riscos simultaneamente. De acordo com Nobrega *et al*., (2014), esse tipo de análise é pouco realizado, porém pode ser muito útil. A análise complementar que pode ser realizada pelos gestores segue os modelos mostrados nas Tabelas 4 e 5.

Tabela 4 - Lista de Probabilidade Simultânea. Nobrega *et al.,* (2014).

Lista de Probabilidade Simultânea								
	Risco 1	Risco 2	Risco 3	Risco 4	Risco 5	Risco 6	Risco 7	Risco 8
Risco 1								
Risco 2	5%							
Risco 3	1%	%						
Risco 4	1%	5%	%					
isco 5	%	%	,55%	,1%				
isco 6	2%	%	%	,1%	,6%			
isco 7	%	%	,23%	,5%	,1%	,3%		
isco 8	%	%	,47%	,9%	,1%	,5%	,0%	

Tabela 5 - Lista de Impacto Simultâneo. Nobrega *et al.*, (2014).

Lista de Impacto Simultâneo								
	Risco 1	Risco 2	Risco 3	Risco 4	Risco 5	Risco 6	Risco 7	Risco 8
Risco 1								
Risco 2	$ 546,00							
Risco 3	$ 25,68	$ 529,68						
Risco 4	$ 2.271,00	$ 2.775,00	$ 2.254,68					
Risco 5	$ 126,00	$ 630,00	$ 109,68	$ 2.355,00				
Risco 6	$ 97,50	$ 601,50	$ 81,18	$ 2.326,50	$ 181,50			
Risco 7	$ 23,25	$ 527,25	$ 6,93	$ 2.252,25	$ 107,25	$ 78,75		
Risco 8	$ 156,00	$ 660,00	$ 139,68	$ 2.385,00	$ 240,00	$ 211,50	$ 137,25	

Na lista de probabilidade simultânea (Tabela 4), deve-se elaborar uma lista visando colocar os riscos nas linhas e colunas, procedendo a seguinte análise para cada relacionamento: para a probabilidade dos riscos 1 e 2 acontecerem simultaneamente, o resultado será a multiplicação das suas probabilidades. Este cálculo será feito para cada um dos relacionamentos. No caso dos impactos (Tabela 5), deve-se fazer o somatório dos valores esperados para cada um dos riscos visando a identificação do impacto da ocorrência de dois riscos simultâneos.

As células com cor de fundo preto representam um relacionamento que já foi representado em outro plano cartesiano. A prioridade é das colunas, seguindo uma ordem da esquerda para a direita. Para que a tabela não possua informações repetidas, utiliza-se o fundo preto.

Após as análises, o gerente deverá criar uma lista de prioridades (Tabela 6). Nesta lista, o gerente deverá identificar qual risco tem prioridade no relacionamento entre eles.

Tabela 6 - Lista de Prioridades. Nobrega *et al.*, (2014).

Lista de Prioridades								
	Risco 1	Risco 2	Risco 3	Risco 4	Risco 5	Risco 6	Risco 7	Risco 8
Risco 1								
Risco 2								
Risco 3								
Risco 4								
Risco 5								
Risco 6						6		
Risco 7								
Risco 8								

A análise deve ser feita de maneira semelhante ao exemplo que utiliza os riscos 1 e 2. Caso o risco 2 seja de maior prioridade em relação ao risco 1, será colocado na célula de relacionamento o número 2 que irá representar o risco 2. O fundo preto da Tabela 6 possui a mesma função apresentada para as Tabelas 4 e 5.

5 ESTUDO DE CASO

Este capítulo apresenta o estudo de caso avaliado em empresa real, com suas respectivas simulações e cenários.

5.1 PLANEJAMENTO DO ESTUDO DE CASO

Foram empregados como base para o princípio do estudo de caso (vide Figura 44), a causa (satisfação dos sujeitos ao utilizar o modelo) e o efeito (análise de preferência, utilidade, completude, efetividade), além da observação do experimento, onde as variáveis independentes (problema a ser resolvido para identificação de pontos críticos passíveis de redundância em redes ópticas) são entradas para a saída do processo (análise da satisfação dos gestores ligados ao gerenciamento de serviços e gerenciamento de redes quanto aos efeitos do modelo - preferência, utilidade, completude, efetividade).

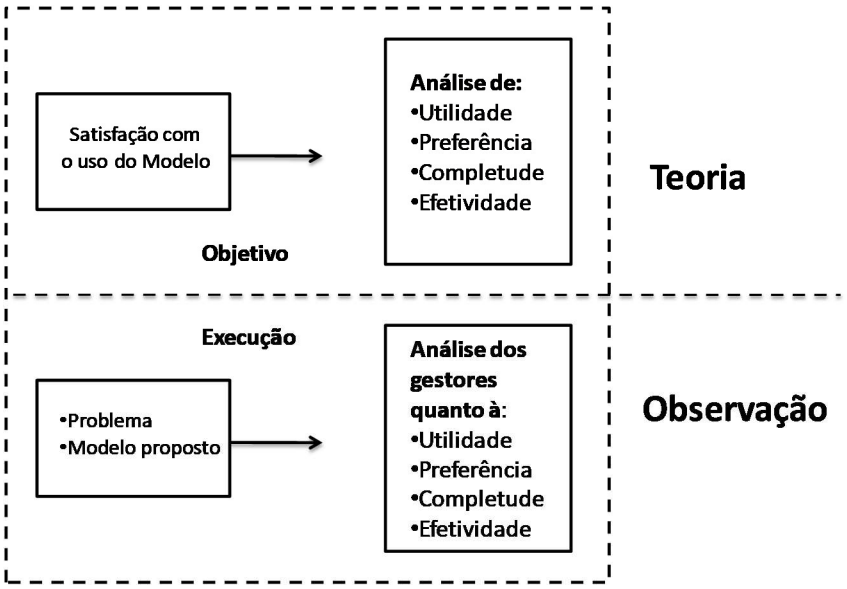


Figura 44. Princípio do Estudo de Caso. Lima *et al.*, (2011).

De acordo com Lima (2011), as pesquisas com utilização de questionários são provavelmente o método de pesquisa mais utilizado em todo o mundo. O trabalho de levantamento é visível, não apenas pelo fato de existirem vários exemplos de pesquisa, mas também porque muitas vezes se é convidado a participar de pesquisas sobre a visão particular, como eleitores, consumidores ou usuários de serviços. Esta ampla utilização de pesquisas pode levara uma falsa impressão de que a investigação baseada em entrevistas ou questionários é

simples, uma opção fácil para os pesquisadores reunirem informações importantes sobre os produtos, o contexto, processos, os trabalhadores e muito mais.

Foram realizados os seguintes tipos de validação para os questionários, seguindo as recomendações de Runerson e Host (2009):

- *validade da aparência* - realizou-se um teste de validade com usuários que nunca tinham visto o questionário, e eles entenderam o que havia sido informado nas questões;
- *validade de conteúdo* - foram feitas entrevistas com especialistas em GSTI - Gerenciamento de Serviços de TI (ou Gestão de Serviços de Informática), do inglês *IT Service Management* (ITSM) e os questionários foram apresentados, junto com seus objetivos, e os mesmos foram considerados adequados para a pesquisa em termos gerais, e algumas correções foram feitas para deixar o texto mais claro;
- *validade de critérios* - fez-se comparações dos questionários com o questionário que já era aplicado para medir a satisfação do usuário, tendo-se constatado que o questionário desta pesquisa foi considerado de fácil entendimento e
- *validade da construção* - convergente. Os questionários projetados possuem características adequadas.

Lima (2011) afirma que a análise de dados transforma a informação em conhecimento de eventos que estão afetando a organização. Para execução de uma análise de dados, é necessário se ter perfil e conhecimento maiores do que para sua coleta e processamento. A confrontação com as metas e objetivos é esperada nessa atividade, para validação do suporte aos objetivos. A produção de gráficos de vários tipos não é suficiente, já que a documentação das observações e conclusões é necessária (OGC, 2007).

Para que se pudesse fazer uma análise da eficiência do *ASP*, foram desenvolvidos para o sistema de localização de falhas módulos probabilísticos. Esses trabalham com os alarmes que são enviados, bem como com os componentes indicados pelo *ASP* por serem os responsáveis pelos alarmes.

5.2 DESCRIÇÃO E ANÁLISES

A presente tese envolve a proposta de um modelo para identificação de pontos críticos em redes ópticas, com base em simulações de cenários e no risco para o negócio. Os resultados obtidos contribuem para a pesquisa na área de gerenciamento de serviços e *BDIM (Business-driven IT Management)*.

Para avaliação do modelo proposto, utilizou-se um problema dimensionado para permitir um tratamento das simulações de cenários de redes ópticas em um contexto real, tendo sido realizado com profissionais que vivenciam no seu cotidiano o gerenciamento de falhas. O foco da avaliação consiste no modelo proposto. O problema foi dimensionado para possibilitar que fosse realizado um tratamento acadêmico, com escopo na avaliação de cinco cenários de redes ópticas de referência na empresa avaliada.

O estudo de caso realizado envolveu uma empresa do segmento de telecomunicações, com sede na cidade de Fortaleza – CE - Brasil. Por razões relativas ao sigilo do negócio, conforme solicitado pela empresa, será referenciada nesta pesquisa como empresa *Alpha*.

A *ferramenta de software ASP*, a qual implementa o modelo proposto nesta tese, foi utilizada pelos gestores, com o objetivo de fornecer suporte às atividades relacionadas aos processos de gerenciamento de incidentes e gerenciamento de falhas, apoiando a tomada de decisão relativa à escolha de quais pontos de rede necessitam de intervenções - incluindo a criação de medidas de redundância. Foram simulados cinco cenários de redes de referência (ARPA2NET, NFSNet, Cost239, USnation e ER_NET), em cinco simulações avaliadas durante esta pesquisa.

As saídas do modelo *ASP* foram apresentadas e validadas junto aos gestores da empresa *Alpha*, com resultados promissores, conforme será mostrado na sequência. A pesquisa envolveu a realização das simulações, além de um processo de validação criterioso e detalhado junto aos gestores de TI e redes que participaram da pesquisa. Questões relacionadas ao tempo, escopo, financiamento do projeto, e principalmente o acesso limitado à população de gestores com o perfil necessário para a avaliação de um modelo com as características do modelo proposto, limitaram a realização de um maior número de repetições.

A população de interesse do estudo contemplou o grupo denominado especialistas do negócio (11 gestores de TI e 6 administradores de redes), no caso os profissionais responsáveis

por decidir como são gerenciados os serviços de TI e redes. A definição da amostra foi realizada por meio de um método não probabilístico, por conta dos sujeitos serem amostras muito específicas e com disponibilidade limitada.

A infraestrutura de TI é responsável por armazenar e disponibilizar todas as informações necessárias para as pessoas certas, da maneira correta e na hora certa. A indisponibilidade de serviços de rede é um dos riscos mais sérios de uma infraestrutura de TI. Quando ocorre, pode deixar vários usuários ou mesmo empresas inteiras sem acesso aos seus serviços principais, afetando diretamente a produtividade, comprometendo a produção, as vendas e a entrega de seus produtos e serviços. A confiabilidade da rede pode ter um impacto direto nos resultados do negócio. Uma falha pode comprometer a segurança de dados e até a continuidade do negócio. Uma falha de rede em um momento crítico afeta o desempenho do negócio.

Ao determinar o *Valor de Risco Esperado (ERV)* para os elementos da rede, a probabilidade de falha para o elemento *e*, *e* = 1,2 ..., E e o grau de relevância de cada elemento para o negócio (muito alto - alto - médio - baixo - muito baixo), usado para estimar o impacto de um elemento de rede, foram obtidos a partir da experiência dos gestores, nos cenários avaliados (esses valores também podem ser derivados de dados reais, obtidos dos registros de cada rede e histórico de uso, se disponíveis). Conforme demonstrado anteriormente, a estimativa de impacto de um elemento de rede é influenciada pelo número de alarmes (identificados pela ferramenta *ASP*) e sua relevância comercial. Modelo *ASP* estima o risco (*ERV*) para cada elemento da topologia da rede óptica. Para o cálculo do *ERV*, assume-se o impacto da falha de um elemento (Expressão 1), onde o valor esperado do risco é calculado multiplicando sua probabilidade de ocorrência com seu grau de impacto. Os valores das probabilidades de falha estimadas para os elementos de rede no estudo de caso são mostrados na Figura 45. Os resultados para cada cenário simulado (vide Tabela 8) são apresentados e analisados a seguir.

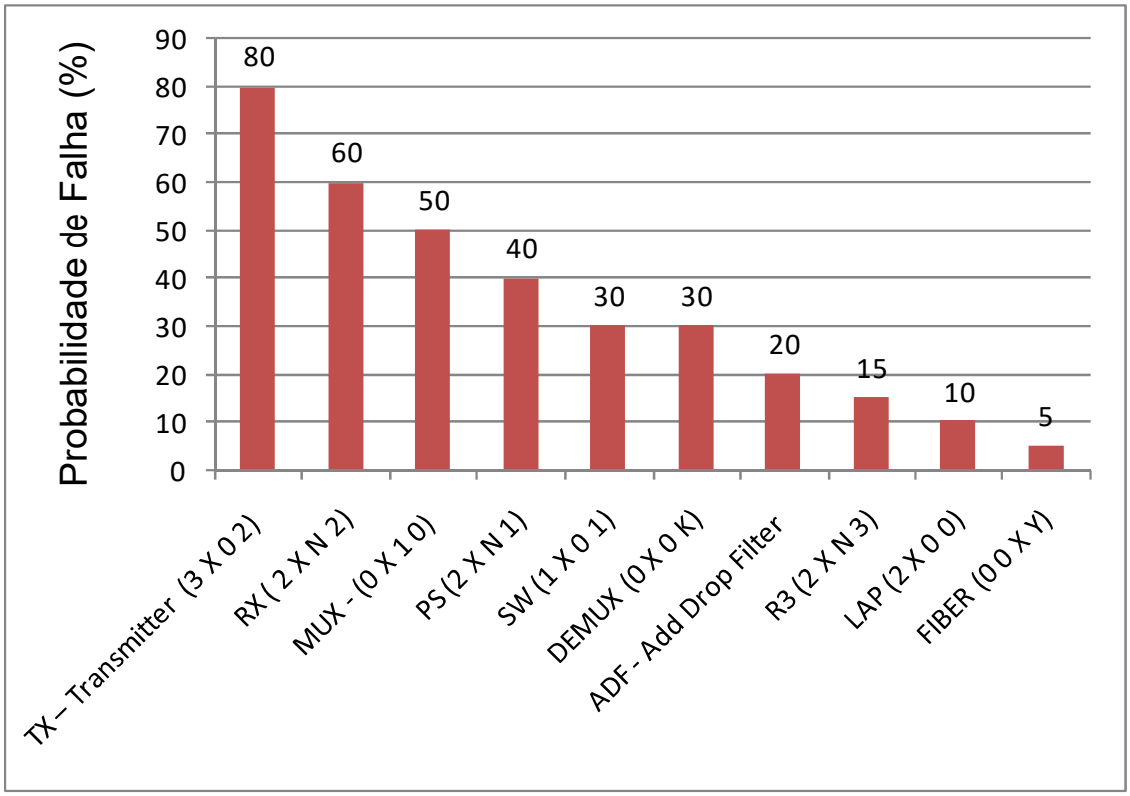


Figura 45. Probabilidades de Falhas (em porcentagens) para elementos da rede para o estudo de caso. Elaborado pelo autor.

Tabela 8 - Cenários simulados no estudo de caso. Elaborado pelo autor.

Categoria do Elemento de Rede	Classe	Relevância para o Negócio	Cenário # 1 ARPA2		Cenário # 2 NFSNet		Cenário # 3 Cost 239		Cenário # 4 Usnation		Cenário # 5 ER_NET	
			Qt	Alarme	Qt.	Alarms	Qt.	Alarms	Qt.	Alarms	Qt.	Alarms
Fibers	P	Very High	20	90	19	69	11	39	28	96	27	81
LAP	P	Medium	12	0	10	0	10	0	7	0	10	0
Demultiplexers	P	Medium	10	45	8	24	3	12	7	24	8	24
Multiplexers	P	High	7	51	5	27	3	15	7	27	6	21
AddDropFilter	A1	High	11	65	10	61	8	41	19	103	23	95
Transmitters	A3	Medium	20	80	11	44	7	28	13	52	12	48
Receivers	A2	Very Low	20	25	11	10	7	10	13	18	12	16
Switches	A1	Very High	7	7	5	5	4	4	7	7	6	6
Protection Switches	A2	Low	20	30	11	16	7	8	13	16	12	16
3R amplifiers	A2	Very Low	20	5	10	3	7	2	13	5	12	4

Conforme citado anteriormente, no estudo de caso realizado, foram avaliadas duas formas de cálculo para o impacto de um elemento de rede para o negócio e sua influência no valor de risco (*ERV*), cujos resultados são comparados na seção de análise de resultados do quinto cenário da presente tese. A Tabela 9 e Figura 46 apresentam os valores utilizados pelos gestores da empresa *Alpha* para o tempo médio entre falhas (*MTBF*) e tempo médio para reparo (*MTTR*) dos elementos de rede nos cenários simulados. Por sugestão dos gestores, os dados desses parâmetros de simulação foram baseados em estatísticas reais da rede óptica gerenciada pela empresa *Alpha*. Entretanto, convém ressaltar que esses dados podem variar bastante, dependendo do tipo de elemento, da estrutura da empresa, da abrangência, da localização, da forma como a rede óptica se encontra implantada, bem como da estrutura e estratégia de manutenção de cada empresa. Esses fatores podem influenciar, por exemplo, que um elemento de rede com baixa probabilidade de falha apresente um alto impacto de reparo (Ex: Fibra na Tabela 9), por conta de interrupções periódicas na rede, ocasionadas por fatores externos à empresa.

Tabela 9 - Parâmetros de simulação de cenários no estudo de caso. Elaborado pelo autor.

Elemento	Categoria	Relevância para o Negócio	Probabilidade de Falha	MTBF (dias)	MTTR (dias)	Impacto do Reparo
Fibras	P	5	5	3,5	0,16	0,0457
LAP	P	3	10	365	0,08	0,0002
Demultiplexadores	P	3	30	365	0,13	0,0004
Multiplexadores	P	4	50	365	0,13	0,0004
AddDropFilter	A1	4	20	365	0,13	0,0004
Transmissores	A3	3	80	120	0,15	0,0013
Receptores	A2	1	60	120	0,15	0,0013
Switches	A1	5	30	120	0,1	0,0008
Protetores de Switches	A2	2	40	120	0,1	0,0008
Amplificadores 3R	A2	1	15	120	0,15	0,0013

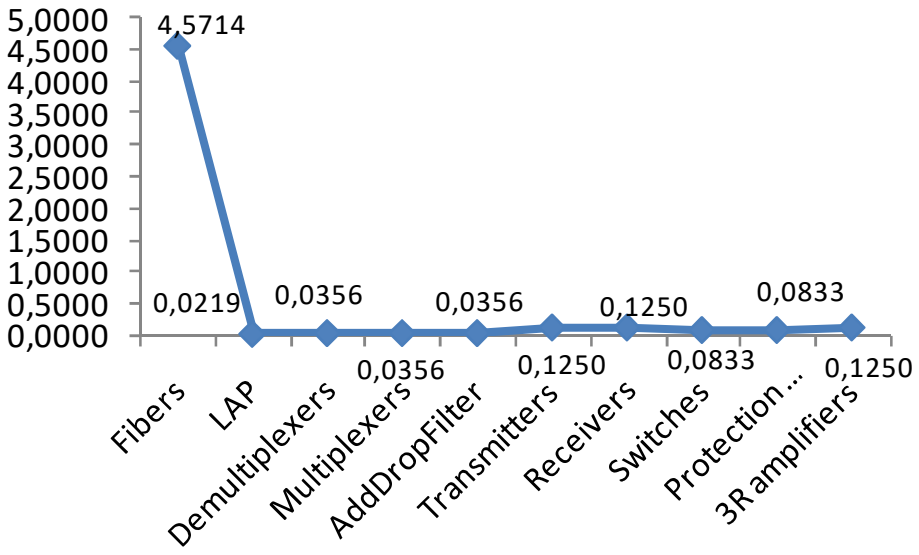


Figura 46. Percentuais de impacto do reparo por elemento de rede. Elaborado pelo autor.

5.2.1.1 Apresentação e discussão dos resultados do Cenário #1

O primeiro cenário de simulação considera uma rede de tipo ARPA2 (ver Figura 47). O cenário simulado contempla rede de referência, amplamente utilizada em simulações de redes na literatura, conforme assevera Lee *et al*., (2011). Foi utilizado como ferramenta de suporte, o *software ASP*, desenvolvido para implementação do modelo *ASP* proposto nesta tese. Sua composição inclui 21 nós, onde 14 são locais e os outros 7 são nós centrais (MAS *et al*, 2000). A Figura 47 mostra uma visão conceitual do cenário avaliado, enquanto a Figura 48 mostra sua implementação por meio do *software ASP*.

Conforme mostrado na Figura 47, os nós representados por um único círculo são nós locais, enquanto os nós representados por dois círculos concêntricos são nós centrais. A rede possui seis canais estabelecidos e quanto maior o número de canais estabelecidos, maior a quantidade de informações enviadas ao gerenciamento, tornando a localização de falhas mais rápida e precisa. As falhas foram intencionalmente introduzidas no cenário avaliado.

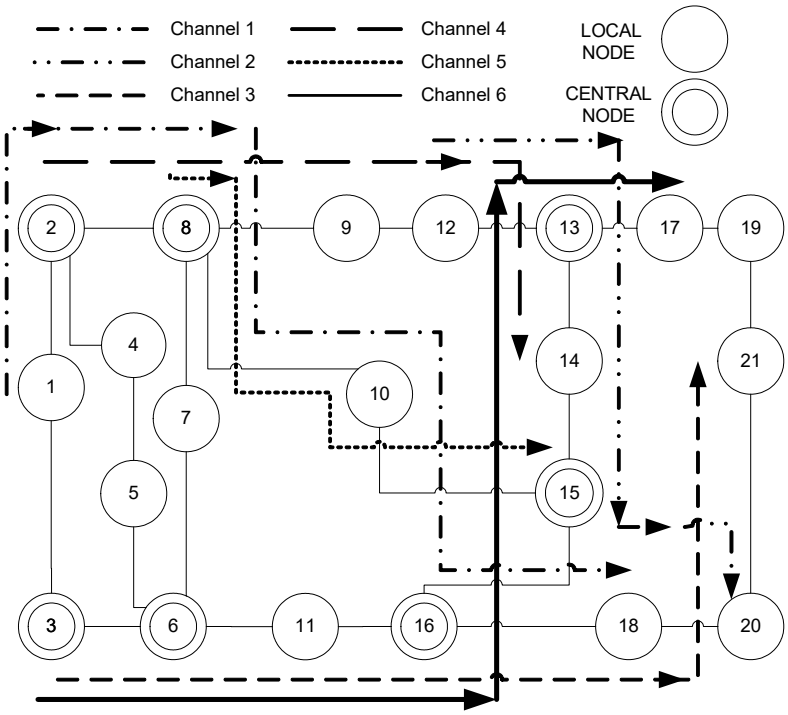


Figura 47. Topologia ARPA2NET. Adaptado de Sousa *et al.*, (2005).

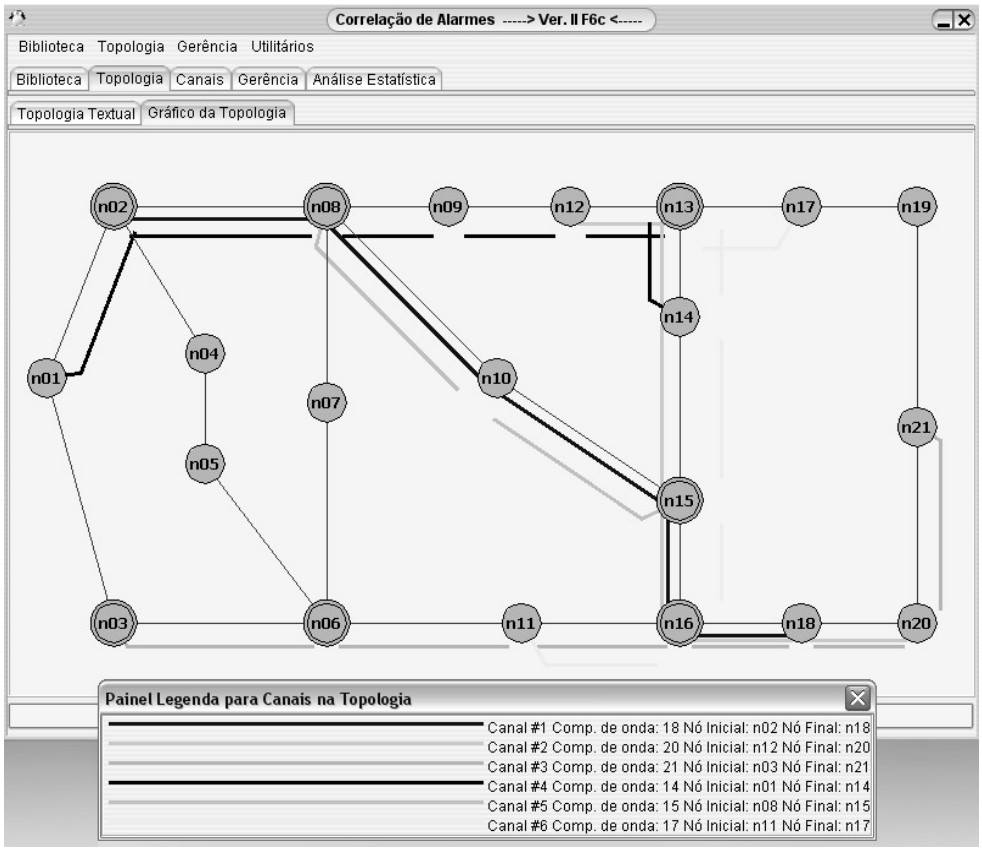


Figura 48. Cenário ARPA2NET no *software ASP*. Elaborado pelo autor através do ASP.

Ao se realizar uma análise a nível de canal, pode ser verificado, como mostrado na Figura 47, que os canais passam por 10 nós locais, 7 nós centrais e 17 *links*. Os parâmetros de simulação de rede ARPA2NET são mostrados na Tabela 8. Há um total de 147 componentes de rede que geram 398 alarmes.

Os canais estabelecidos são formados pelos seguintes nós:

- Canal 1: 2, 8, 10, 15, 16 e 18;
- Canal 2: 12, 13, 14, 15, 16, 18 e 20;
- Canal 3: 3, 6, 11, 16, 18, 20 e 21;
- Canal 4: 1, 2, 8, 9, 12, 13 e 14;
- Canal 5: 8, 10 e 15;
- Canal 6: 11, 16 ,15, 14, 13 e 17.

Para se ter uma noção maior da complexidade do cenário, é mostrada na Figura 49 a topologia em maiores detalhes da rede óptica avaliada.

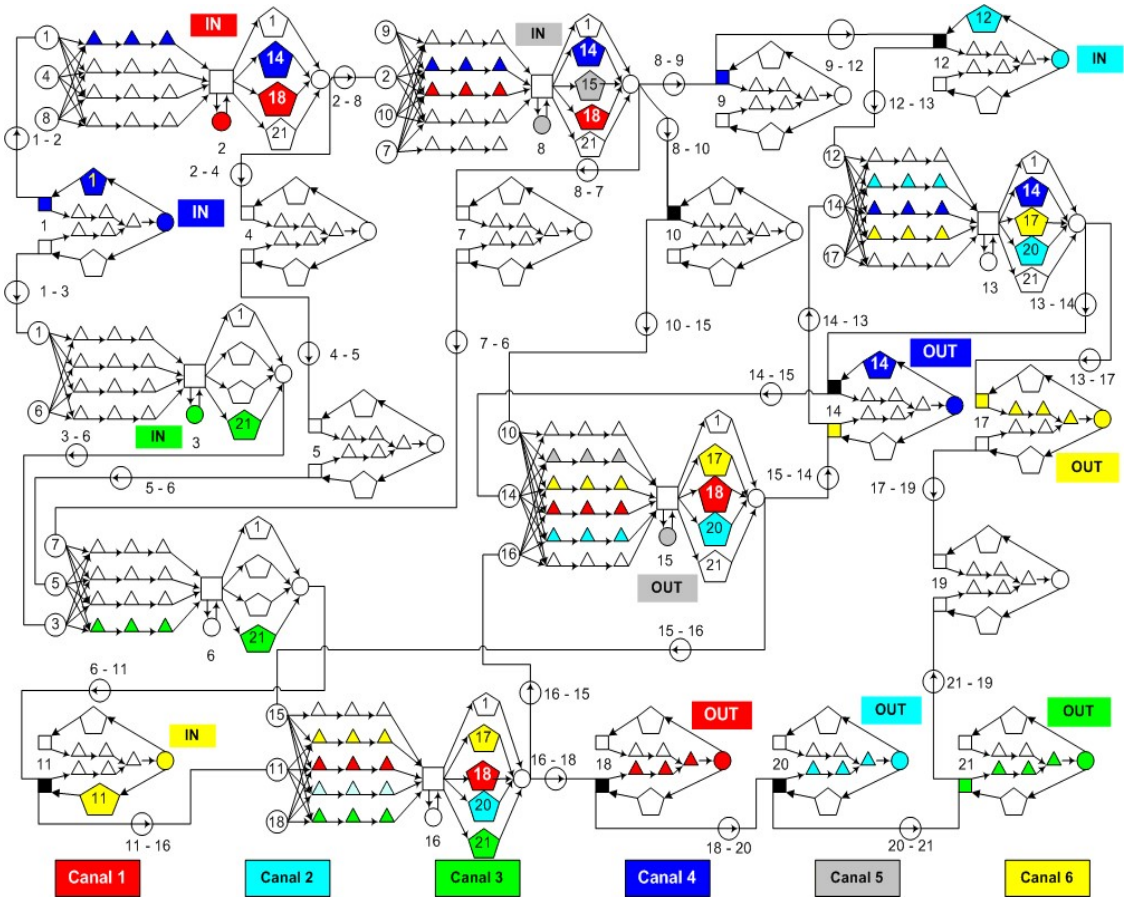


Figura 49. Diagrama ao nível de componentes da rede em malha na topologia ARPA2NET. Elaborado pelo autor.

Analisando a quantidade de componentes em canais separados por classe, temos: 38 do tipo A1, 60 do tipo A2, 20 do tipo A3 e 49 do tipo Passivo.

Ao se realizar o somatório dos componentes pode-se verificar que resultará em 167 componentes. Isso indica que alguns componentes estão sendo utilizados por mais de um canal. Como exemplo temos o comutador do nó 15, ele é compartilhado pelos canais 1, 2 e 5.

Na Figura 50 está representada parte da Figura 49, e é dado enfoque no trecho por onde trafega o canal 5, que inicia no nó central 8, passa pelo nó local 10 e termina no nó central 15.

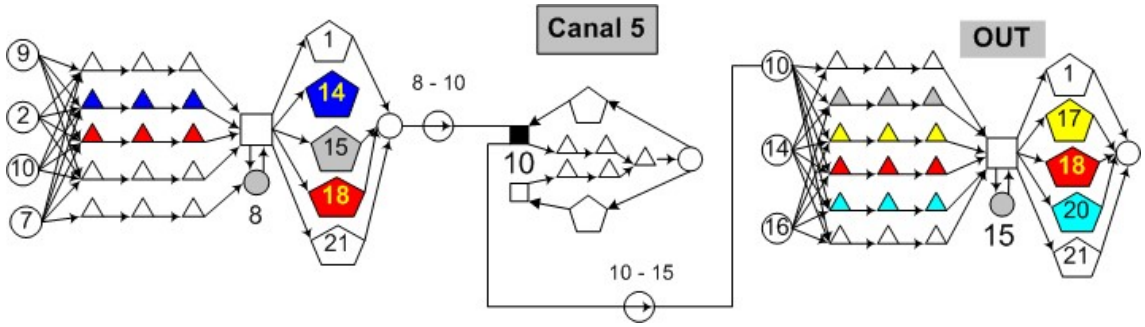


Figura 50. Parte da rede com detalhe nos nós do canal 5. Elaborado pelo autor.

Uma descrição componente a componente do canal 5 é apresentada na Figura 51.

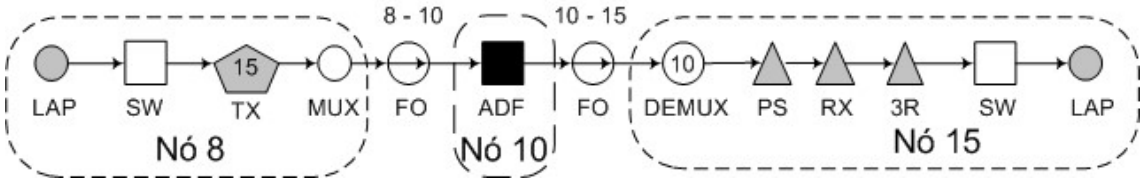


Figura 51. Parte da rede com detalhe nos componentes do canal 5.Elaborado pelo autor.

Pela Figura 51 pode-se listar todos os componentes por onde passa o sinal óptico transportado pelo canal 5. Os componentes são os seguintes:

- Componentes do nó 8: LAP (0 8 0 0) – SW (1 8 0 1) – TX (3 8 0 15) – MUX (0 8 1 0);
- Enlace 8-10: Fibra (0 0 8 10);
- Componentes do nó 10: ADF (1 10 0 1);
- Enlace 10-15: Fibra (0 0 10 15);

- Componentes do nó 5: DEMUX (0 15 0 10) – PS (2 15 15 1) – RX (2 15 15 1) – 3R (2 15 15 1) – SW (1 15 0 1) – LAP (0 15 0 0);

Exemplo 1 - Análise de uma falha na fibra

Falha na fibra entre os nós 16 e 18, identificada por (0 0 16 18). Nesta falha três canais são interrompidos: CH1, CH2, CH3, e os seguintes componentes emitirão alarmes para a gerência: (2 18 0 1) (2 18 0 4) (2 18 0 3) (2 20 0 1) (2 20 0 4) (2 20 0 3) (2 21 0 1) (2 21 0 4) (2 21 0 3). Estes componentes são o PS, 3R e RX (trio de recepção) dos canais interrompidos. Seguindo os passos utilizados pelo *ASP* para a localização da falha temos:

a. Não há componente A1 ou A3 alarmando;
b. Primeiro componente A2 alarmado em cada canal: (2 18 0 1) (2 20 0 1) (2 21 0 1). O percurso inverso até encontrar o primeiro TX em cada canal encontrará os seguintes componentes: CH1: TX (nó 16), MUX (nó 16), fibra (nós 16-18), ADF (nó 18); CH2: TX (nó 16), MUX (nó 16), fibra (nós 16-18), ADF (nó 18), fibra (nós 18-20), ADF (nó 20); CH3: TX (nó 16), MUX (nó 16), fibra (nós 16-18), ADF (nó 18), fibra (nós 18-20), ADF (nó 20), fibra (nós 20-21), ADF (nó 21). Os componentes TX (A3) e ADF(A1) devem ser retirados.
c. Sobram como componentes suspeitos: MUX (nó 16), fibra (16-18), fibra (18-20) e fibra (20-21). Existe um canal passando pelo nó 16 que não está alarmando, o que libera o MUX. Dos três componentes restantes, a fibra (16-18) identificada como (0 0 16 18) é a única que se interrompida apresentaria os alarmes inicialmente analisados.

Como resultado o *ASP* apresentará o componente (0 0 16 18) como suspeito de originar a falha, o que está correto. Como pode ser observado na Figura 52.

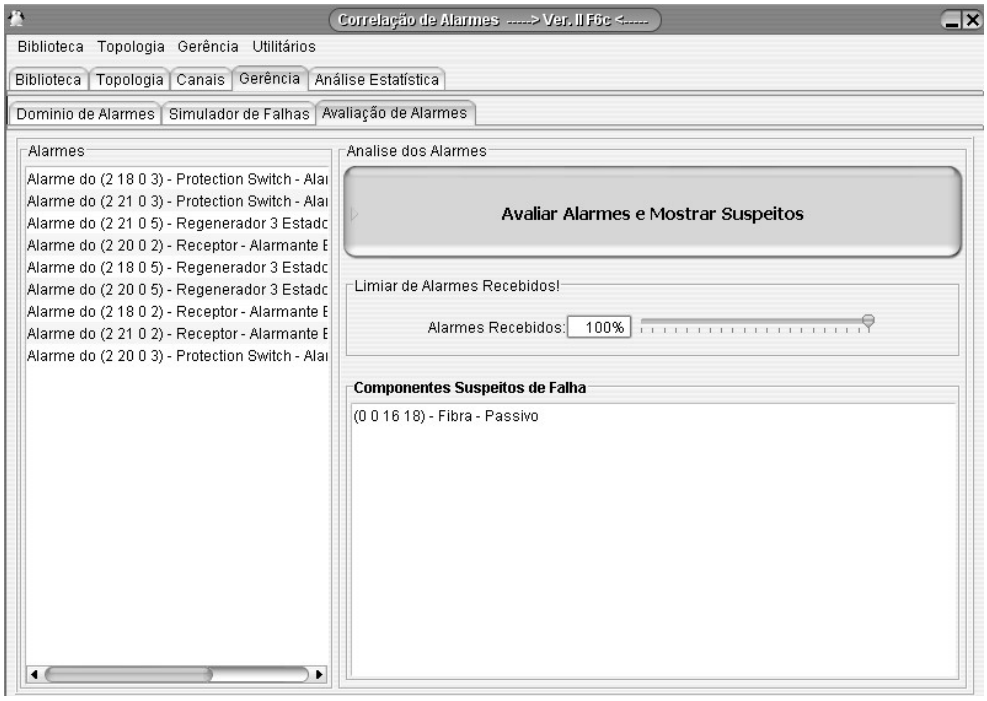


Figura 52. Resultado da análise do ASP obtendo como resultado a fibra entre os nós 16 e 18. Elaborado pelo autor através do ASP.

Exemplo 2 - análise de uma falha em um transmissor

Considerando uma falha no transmissor do nó 6, onde trafega o canal 3. Os alarmes que devem ser enviados são os seguintes: (3 6 0 21) (2 16 21 1) (2 16 21 2) (2 16 21 3). Contudo, somente os seguintes alarmes foram enviados para a gerência: (2 16 21 1) (2 16 21 2) (2 16 21 3). Seguindo os passos do *ASP* tem-se:

a. Não há componente A1 ou A3 alarmando;
b. Primeiro componente A2 alarmado: (2 16 21 1) PS (nó 16). Os componentes localizados entre ele e o primeiro TX: TX (nó 6), MUX (nó 6), fibra (nós 6-11), ADF (nó 11), fibra (nós 11 -16), DEMUX (nó 16). Destes, os componentes TX (A3) e FDI (A1) são retirados.
c. Tem-se então como suspeitos: MUX (nó 6), fibra (nós 6-11), fibra (nós 11 -16), DEMUX (nó 16). Como a fibra (nós 11 -16) e o DEMUX (nó 16) estão sendo utilizados pelo nó 6 e este não está alarmando, eles serão liberados.

Então o *ASP* apresenta como resultado pelos alarmes gerados o MUX (nó 6) e a fibra (nós 6-11), como pode ser observado na Figura 53.

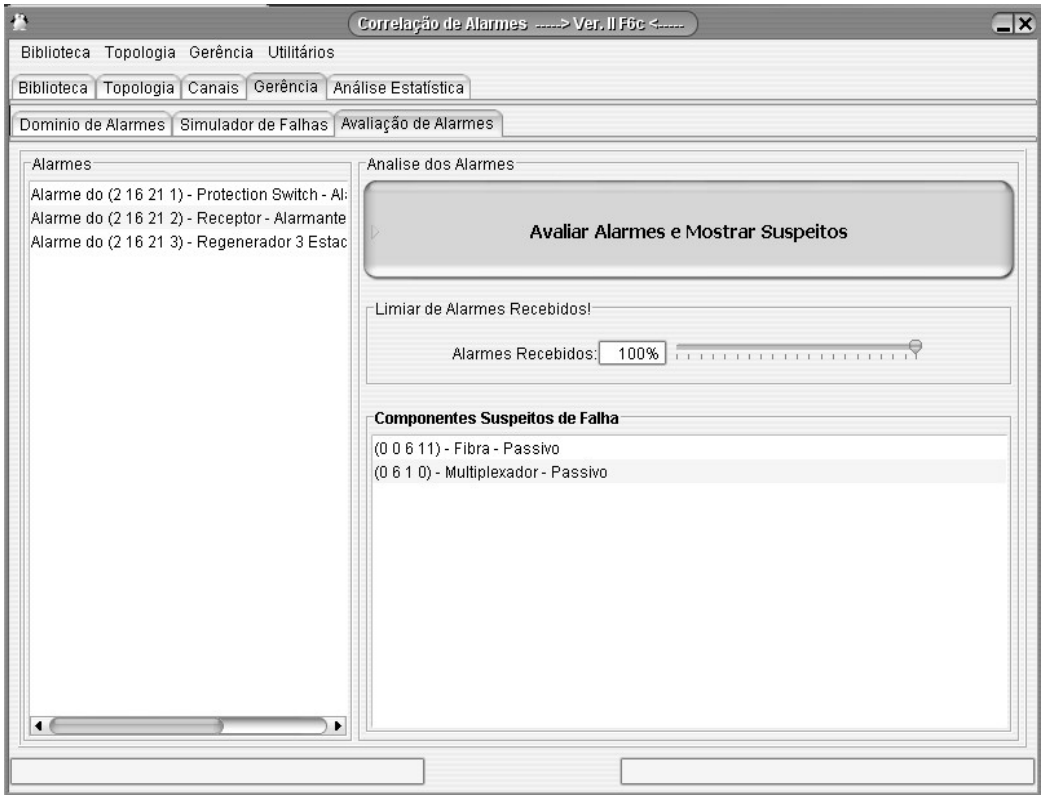


Figura 53. Resultado da análise do *ASP* obtendo como resultado a fibra entre os nós 6 e 8, além do multiplexador do nó 6. Elaborado pelo autor através do ASP.

Analisando o resultado dos dois cenários de falhas podemos observar que para o primeiro caso o *ASP* obteve um resultado relativo à identificação de falha, superior ao AFA-FLA (MAS. *et al*., 2000), *Alarm Filtering Algorithm-Fault Location Algorithm*, pois o mesmo considerou além da fibra entre os nós 16 e 18, que o multiplexador do nó 16 era um componente suspeito. Contudo, no segundo caso o *AFA-FLA*, conforme confrontação com dados obtidos em Mas. *et al.,* (2000), apresentou o resultado correto, enquanto o *ASP* apresentou dois suspeitos inocentes. Em termos gerais, o módulo de identificação de falhas do *software ASP*, desenvolvido a partir de extensão da pesquisa do autor desta tese (SOUSA *et al*., 2005), apresentou um resultado superior. Na sequência, serão descritos os aspectos relacionados ao negócio, que direcionam a solução proposta nesta pesquisa.

Para o cálculo do *Valor de Risco Esperado (ERV)*, assume-se o risco de um elemento (*e*) ser dado multiplicando a sua probabilidade de ocorrência (P_e) com seu grau de impacto (ou seja) no negócio (ver Expressão 14).

$$ERV_e = P_e \; x \; i_e \qquad (14)$$

Como informado anteriormente, o modelo *ASP* é flexível e os gestores podem escolher equações diferentes para estimar o impacto do elemento da rede (i_e). Em um trabalho futuro, o plano é construir uma "biblioteca de possíveis equações" (considerar, por exemplo, perfil de risco da empresa, variação de risco ao longo do tempo, procedimentos de mitigação, idade da infraestrutura, etc.) para estimar o impacto do elemento.

No estudo de caso realizado na empresa *Alpha*, a opção dos gestores foi simplificar a estimativa de impacto, ilustrar o uso do modelo e coletar possíveis evidências de que o modelo funciona e é útil. Usando a abordagem baseada em consenso (com base no método *Delphi*), foi realizada a estimativa de relevância pelos gestores para cada elemento da rede óptica.

Como mostrado anteriormente na apresentação do modelo *ASP*, o impacto do elemento de rede, ou seja, $i_e = \{1,2, \ldots E\}$ - E é o total dos elementos, é calculado (reiterado nas equações 7, 8 e 9) pela média ponderada entre a relevância do elemento de rede (Ne_e) soma de alarmes de elemento (Ag_e) multiplicado pela relevância comercial (R_e - um peso), dividido pela relevância total dos alarmes (Ta_e), soma de todos os alarmes gerados multiplicados pela respectiva relevância (pesos). Essa forma de cálculo do impacto do elemento de rede foi utilizada nas simulações dos cenários de 1 a 5, durante o estudo de caso.

O modelo *ASP* permite que a relevância de um elemento de rede possa ser definida para uma categoria de elementos (por exemplo, *Switches*) ou para cada elemento de rede em um nó, de acordo com sua localização na topologia da rede óptica. No estudo de caso, os gerentes da empresa *Alpha* decidiram definir a relevância para o negócio em cenários simulados por categoria de elemento de rede (vide Tabela 8).

A partir da simulação realizada para o primeiro cenário, pode-se observar que a Figura 54 é baseada no *ranking* de risco gerado pelo modelo *ASP* e mostra uma visão de gerenciamento (gráfico de radar) dos elementos da rede óptica ARPA2NET, de acordo com o seu *ERV*. Os elementos mais críticos estão no topo, enquanto os elementos de risco mais baixos estão no centro. Ao decidir sobre a escolha dos pontos de redundância, os gerentes podem analisar toda a tabela de classificação de risco que gerou essa informação.

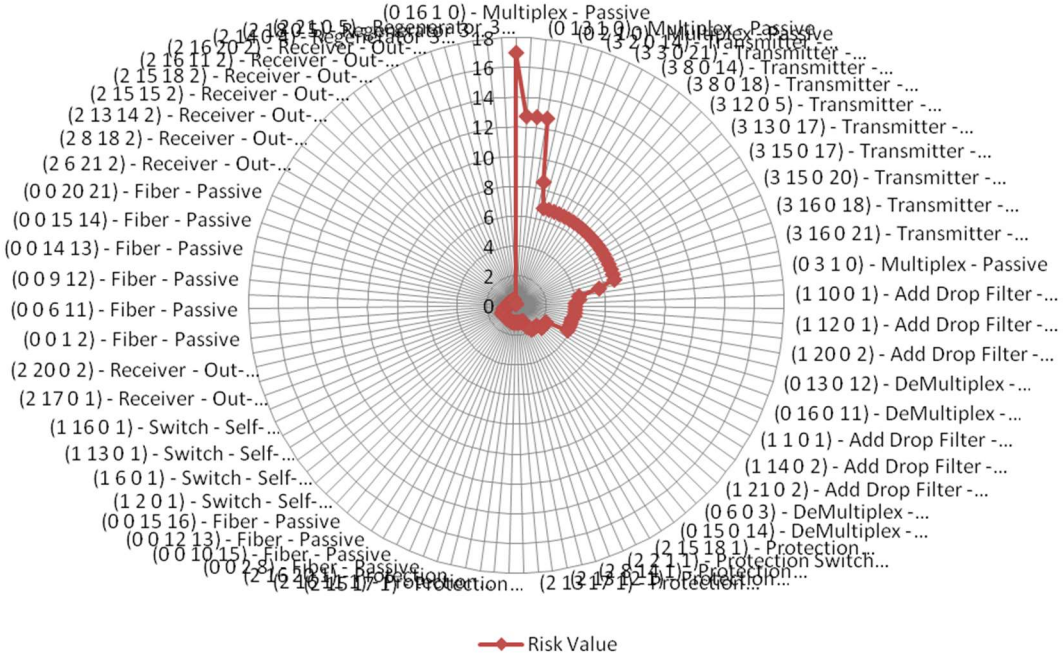


Figura 54. Riscos dos elementos de rede na simulação do primeiro cenário. Elaborado pelo autor através do ASP.

A Figura 55 mostra os riscos relacionados à categoria de elementos da rede do tipo *Fiber* na simulação ARPA2NET. Os gerentes podem observar que a maioria dos valores de risco de elementos da rede do tipo *Fiber* estão localizados em uma zona de risco entre 0,5 e 1. A Fibra que apresenta o maior risco para o negócio, de acordo com as saídas do modelo *ASP*, é o elemento com referência (0 0 16 18), que significa Fibra (0 0), entre os nós 16 e 18.

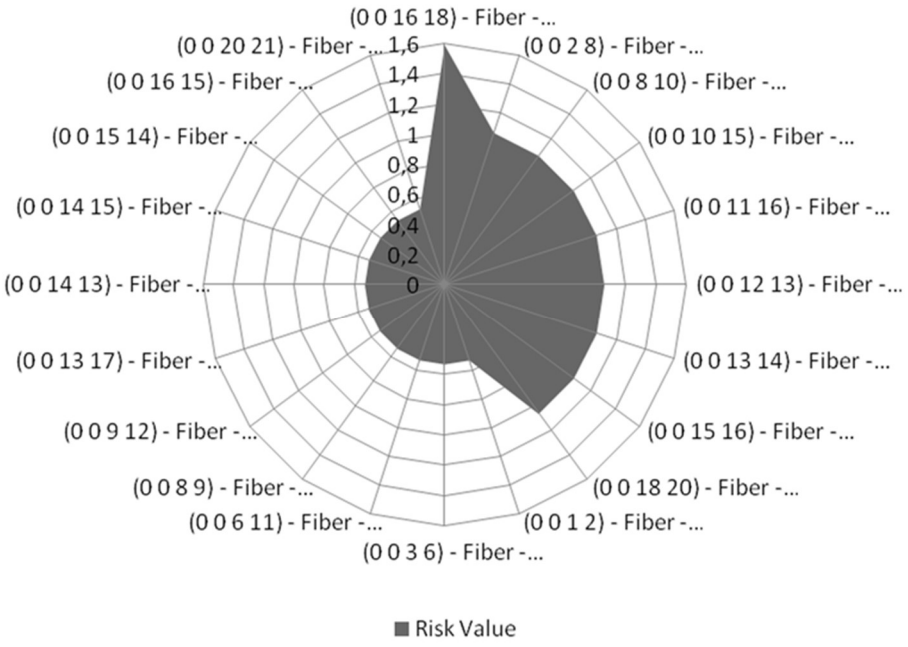


Figura 55. Riscos relacionados a categoria de elemento Fibra. Elaborado pelo autor através do ASP.

A partir dos dados de simulação (vide Figura 54), pode-se observar que o maior risco está relacionado a um Multiplexador em ARPA2NET. Os gerentes podem analisar os dados mostrados na Figura54, para decidir sobre a priorização de redundância de Multiplexadores. O modelo *ASP* pode gerar dados de saída, como os mostrados nas Figuras 54, 55 e 56, relacionadas a todas as categorias de elementos de rede óptica, para apoiar o processo de tomada de decisão.

Os valores de risco relacionados às categorias de elementos ARPA2NET são mostrados na Figura 57. Embora a análise de elementos de simulação indicasse que um Multiplexador era o elemento de rede com maior risco (vide Figura 54), pode-se observar que a categoria com maior risco era Transmissores (veja Figura 57). Os gestores podem usar esses dados como uma informação complementar durante o processo de tomada de decisão.

Quando perguntado sobre a utilidade do modelo *ASP* na identificação de possíveis pontos de redundância nas redes ópticas, os gestores da empresa *Alpha* citaram que os resultados da simulação são muito úteis e podem fornecer um suporte efetivo no processo de tomada de decisão.

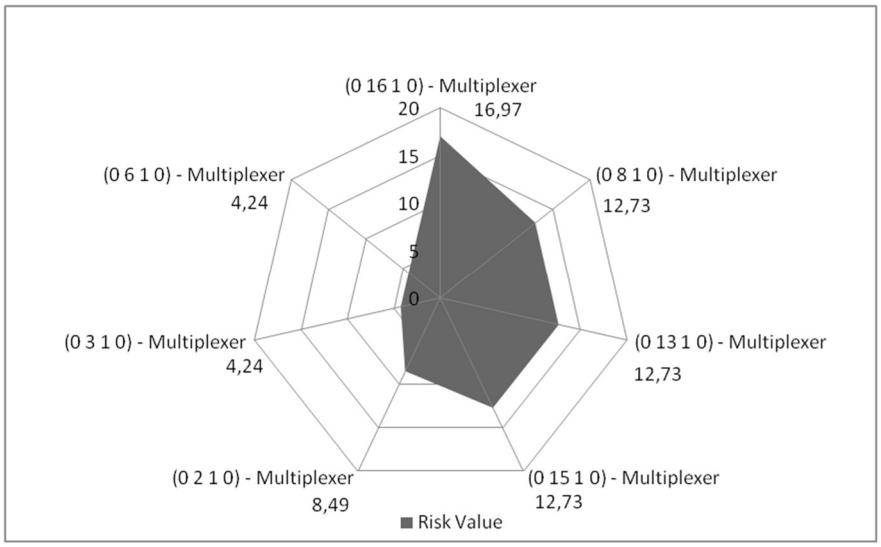


Figura 56. Riscos relacionados a categoria de elemento Multiplexador. Elaborado pelo autor através do ASP.

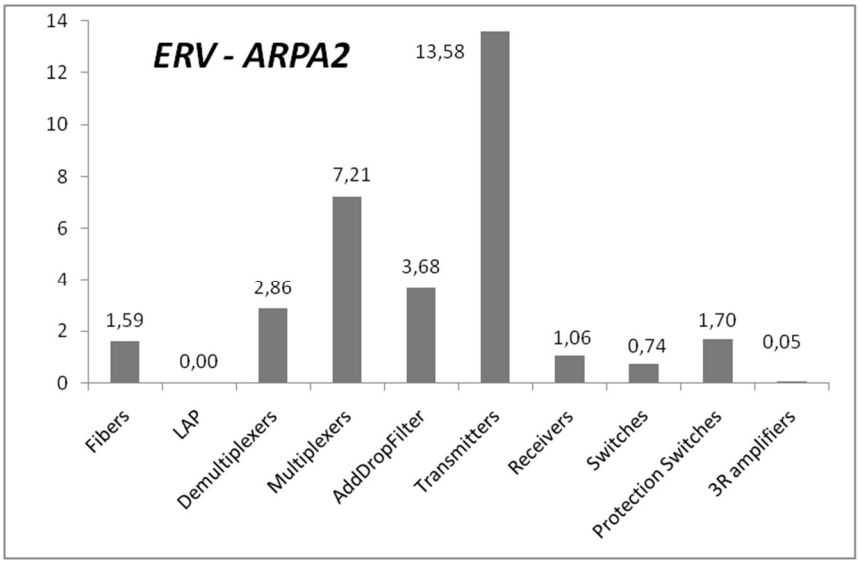


Figura 57. Riscos por categoria de elemento. Elaborado pelo autor através do ASP.

A análise de elementos da simulação do cenário ARPA2NET sinaliza que os demultiplexadores com maior risco na topologia estão localizados nos nós (0 8 0 2), (0 13 0 12), (0 15 0 10), (0 16 0 11) e (0 16 0 15) (vide Figura 58). Os gestores podem usar esses dados como uma informação complementar, em estudos comparativos durante o processo de tomada de decisão.

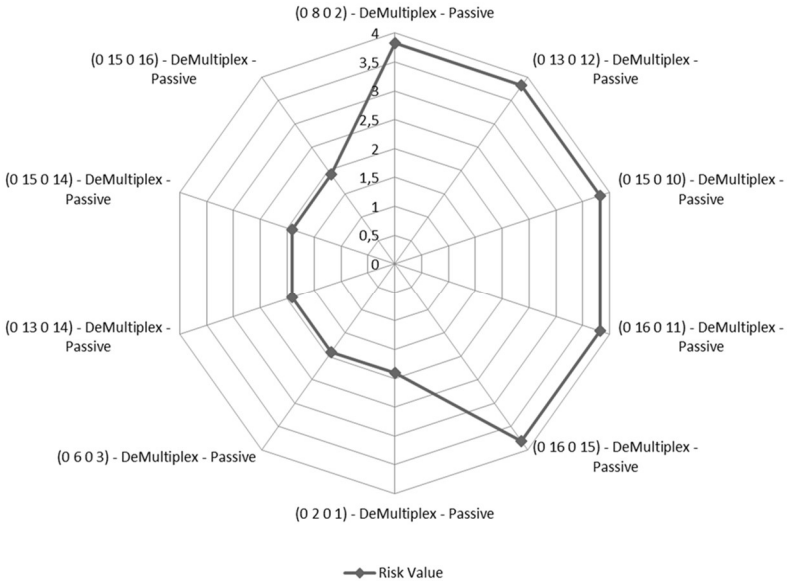


Figura 58. Riscos relacionados a categoria de elemento Demultiplexador. Elaborado pelo autor através do ASP.

Outro ponto interessante que pode ser observado a partir da Figura 59 consiste no fato de que todos os transmissores da topologia ARPA2NET apresentaram o mesmo valor de risco. Somente os multiplexadores apresentaram um valor de risco maior que o identificado para os transmissores no cenário avaliado. Uma análise de impacto em cima do cálculo do risco, pode esclarecer para os gestores maiores detalhes acerca da relação causa efeito que envolve a estimativa.

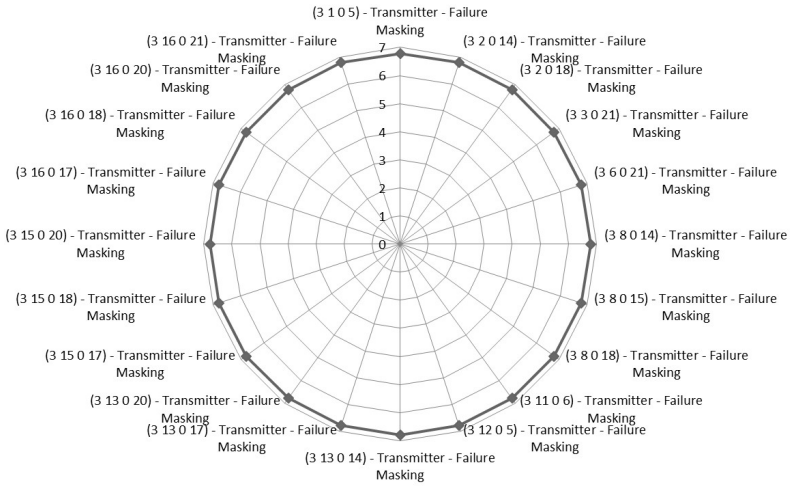


Figura 59. Riscos relacionados a categoria de elemento Transmissor. Elaborado pelo autor através do ASP.

Assim como na análise dos elementos do tipo Fibra, os elementos do tipo ADF apresentaram três diferentes valores de risco na topologia avaliada. Existiu influência da quantidade de canais que passaram pelos nós que contém esses elementos nesse cenário (vide Figura 60)

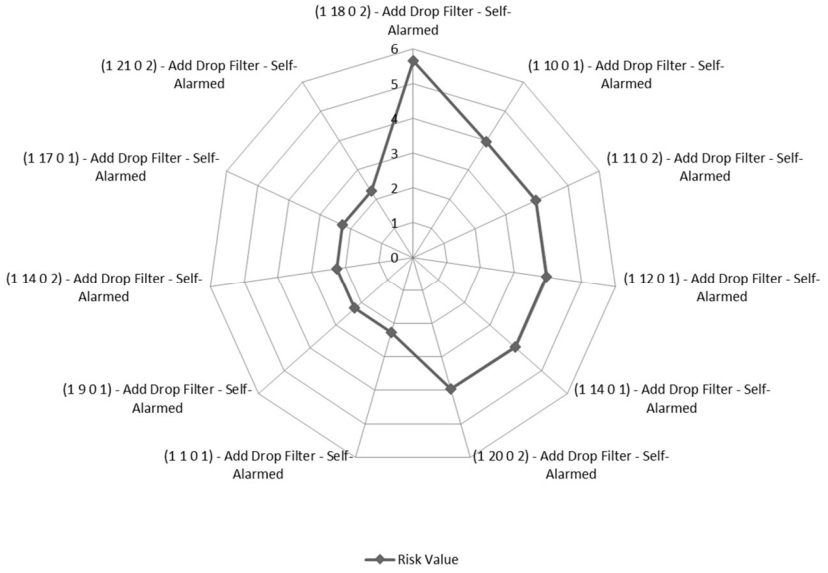


Figura 60. Riscos relacionados a categoria de elemento ADF. Elaborado pelo autor através do ASP.

Os valores de riscos identificados para os elementos *Protection Switch* na topologia avaliada são mostrados na Figura 61. Foi identificado que a zona de risco que envolve a categoria está entre os valores 1,13 e 1,69.

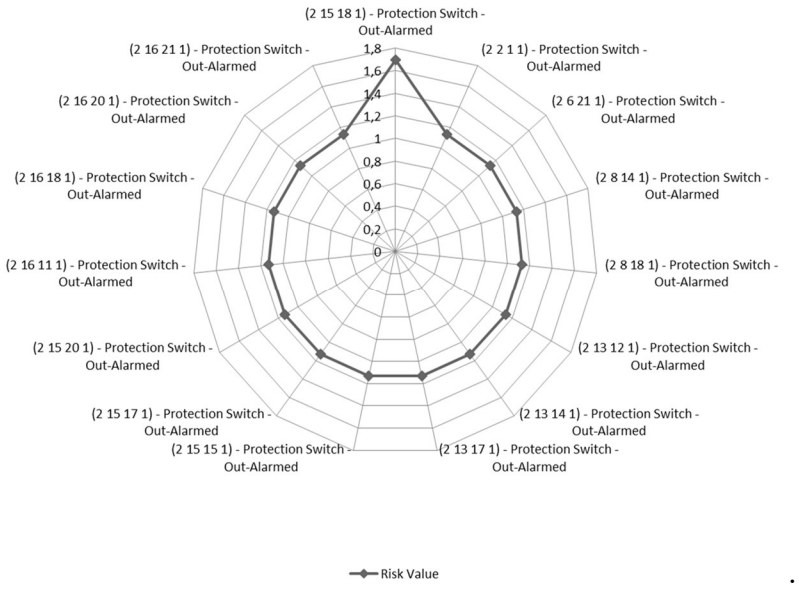


Figura 61. Riscos relacionados a categoria de elemento Protetor da Switch. Elaborado pelo autor através do ASP.

Os valores de riscos identificados para os elementos *Receiver* na topologia avaliada são mostrados na Figura 62. Foi identificado que a zona de risco que envolve a categoria está entre os valores 0,42 e 0,85.

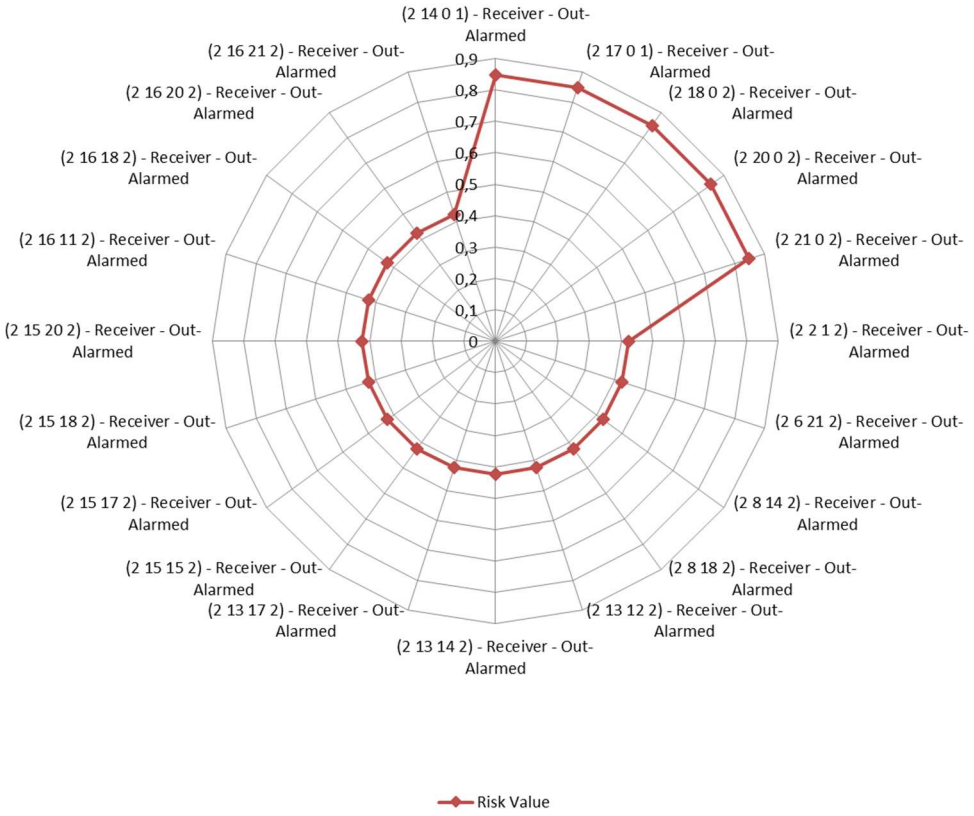


Figura 62. Riscos relacionados a categoria de elemento Receiver. Elaborado pelo autor através do ASP.

São apresentados na Figura 63 os dados para a análise estatística de falhas simples, ou seja, um componente falho por vez para o primeiro cenário. Como pode ser observado, o total de componentes avaliados na rede ARPA2NET foi 115, embora o número de componentes pertencentes a canais seja 147. Isto é justificado pela falta de alarmes quando alguns componentes falham, como por exemplo, os comutadores de proteção dos nós locais finais. Em relação ao campo do tempo, os dados são apresentados em milissegundos. A média de tempo para a análise de cada componente foi de aproximadamente 0,154 segundo e o tempo total da análise de todos os 115 componentes foi de 17,813 segundos. No que diz respeito aos alarmes, eles totalizaram 398, sendo a média de 3,46 alarmes por componente.

Ao se analisar o conjunto dos componentes suspeitos foi verificado que a média foi em torno de 2,026 significando que para cada componente que venha a falhar na rede ARPA2NET o *ASP*, em média, apresentará 2,026 suspeitos para o operador da rede. No máximo serão passados 6 componentes como suspeitos para a apreciação. Visto que a moda é o valor 1, então pode-se admitir que o *ASP* na maioria das vezes encontrou exatamente o componente falho. O

desvio padrão de valor aproximado de 1,314 componentes, indica que a quantidade de componentes suspeitos não difere muito da quantidade de componentes da média.

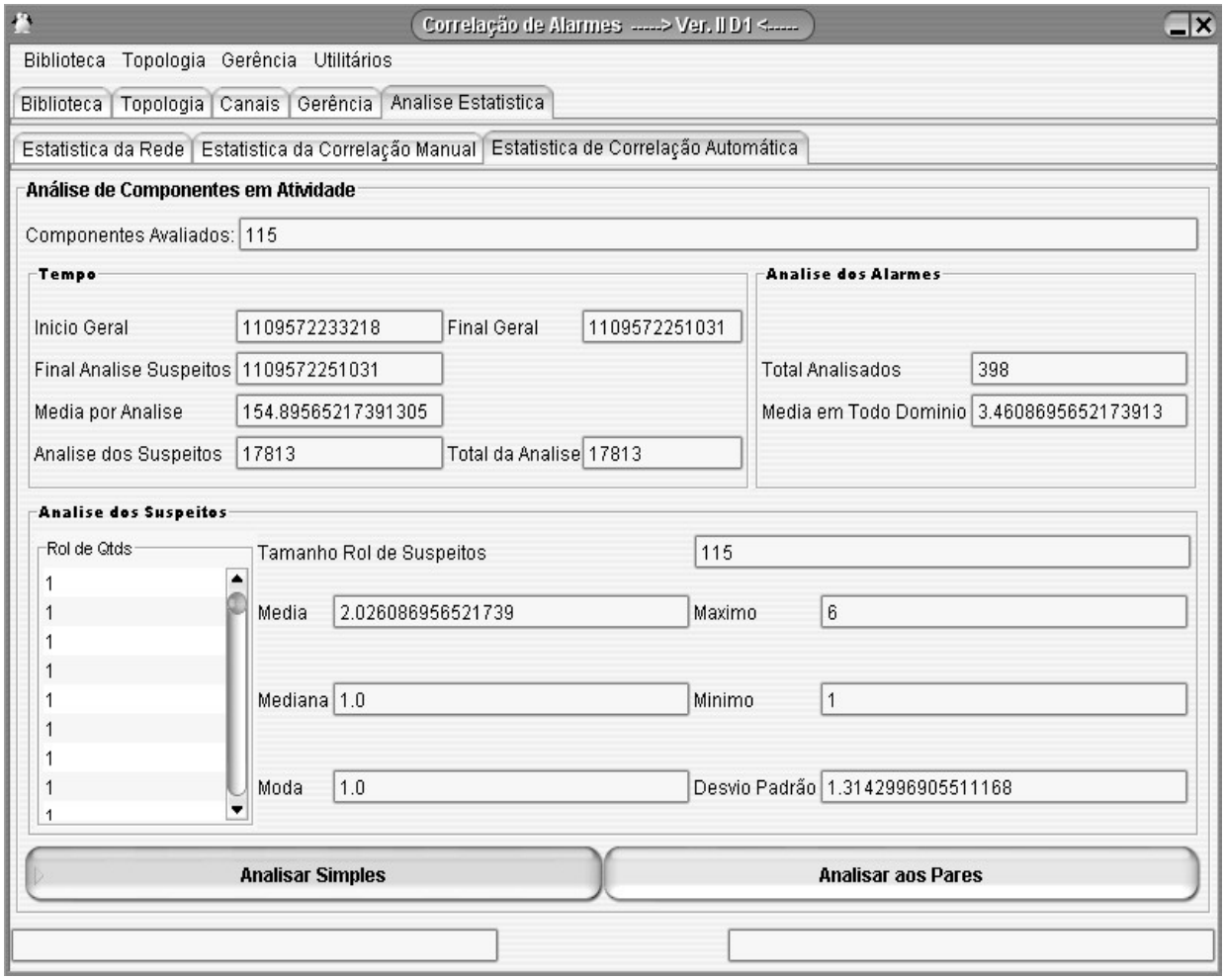


Figura 63. Tela do software *ASP* mostrando dados de validação estatística da simulação da rede ARPA 2. Elaborado pelo autor através do ASP.

5.2.1.2 Apresentação e discussão dos resultados do Cenário #2

O segundo cenário de simulação considera uma rede de tipo NFSNet (Figura 64-a). Sua composição inclui 14 nós, onde 9 deles são locais e os outros 5 são nós centrais. Existem 19 links e 101 elementos de rede.

Os resultados da simulação para o segundo cenário indicaram que os *Multiplexadores* e os *Transmissores* obtiveram valores de risco geral mais elevados na NFSNet (Figura 64-b).

Ao se comparar as informações apresentadas nas Figuras 54 e 64, pode-se observar que no cenário ARPA2NET existe apenas um elemento de rede com maior risco, enquanto que no cenário NFSNet, quatro elementos de rede possuem o maior valor de risco. Isso pode indicar que o segundo cenário tende a exigir um maior investimento em pontos de redundância. O valor de risco dos transmissores foi estimado em 9,89 para todos os elementos de rede, como mostrado na Figura 64.

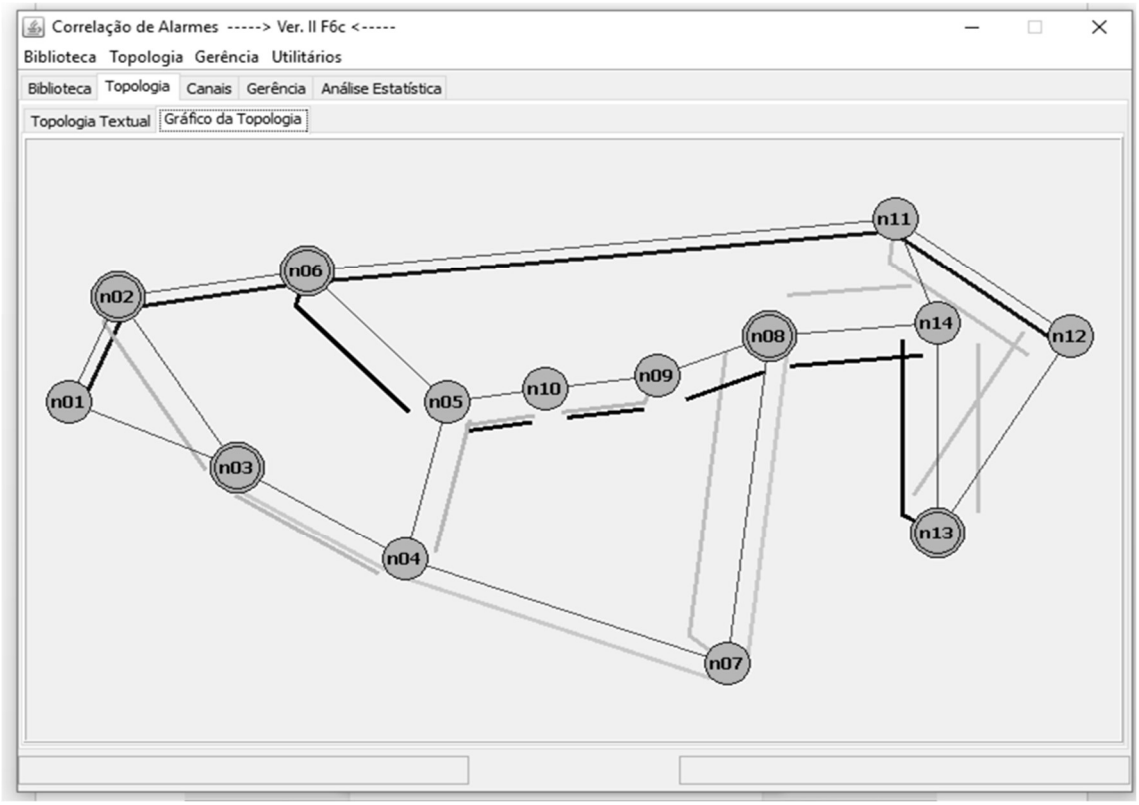


Figura 64-a. Topologia do cenário *NFSNet.* Elaborado pelo autor através do ASP.

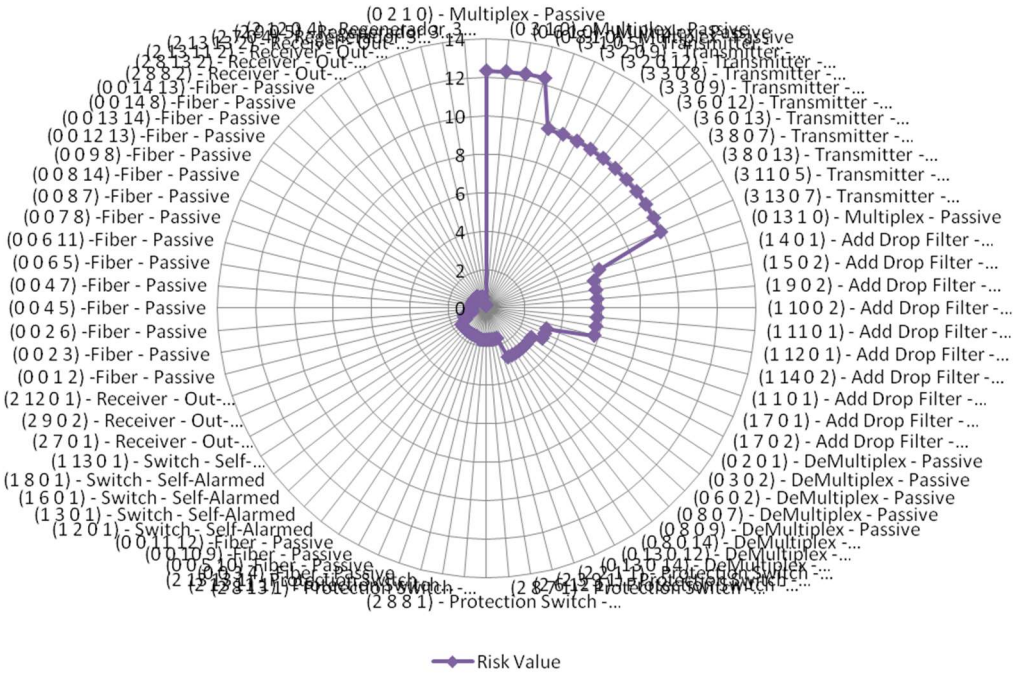


Figura 64-b. Riscos dos elementos de rede na simulação do segundo cenário. Elaborado pelo autor através do ASP.

Na Figura 65, pode-se observar que o risco (*ERV*) para cada elemento de rede foi estimado em uma zona de risco entre 3,3 e 5,77. Os gestores podem avaliar os ADFs com o risco de 5,77 para decidir qual deles receberá redundância. Os níveis de prioridade serão decididos pelos gestores.

A Figura 66 mostra o risco estimado por categoria de elemento de rede óptica, para cenário NFSNet. Se comparado ao cenário *ARPA2NET*, pode-se observar que a categoria *Transmissor* ainda apresenta o maior valor de risco. Essa tendência confirma aos gestores o alto impacto desta categoria de elemento de rede para empresas. Se comparando valores nas Figuras 56 e 66, pode-se observar que o risco relacionado às categorias *Switches* e *Receptores*, mudou devido a possíveis diferenças na topologia e canais dos cenários avaliados. Dessa forma, pode-se identificar que os valores de risco (*ERVs*)estimados pelo modelo ASP são influenciados pela topologia de rede, canais e impacto comercial.

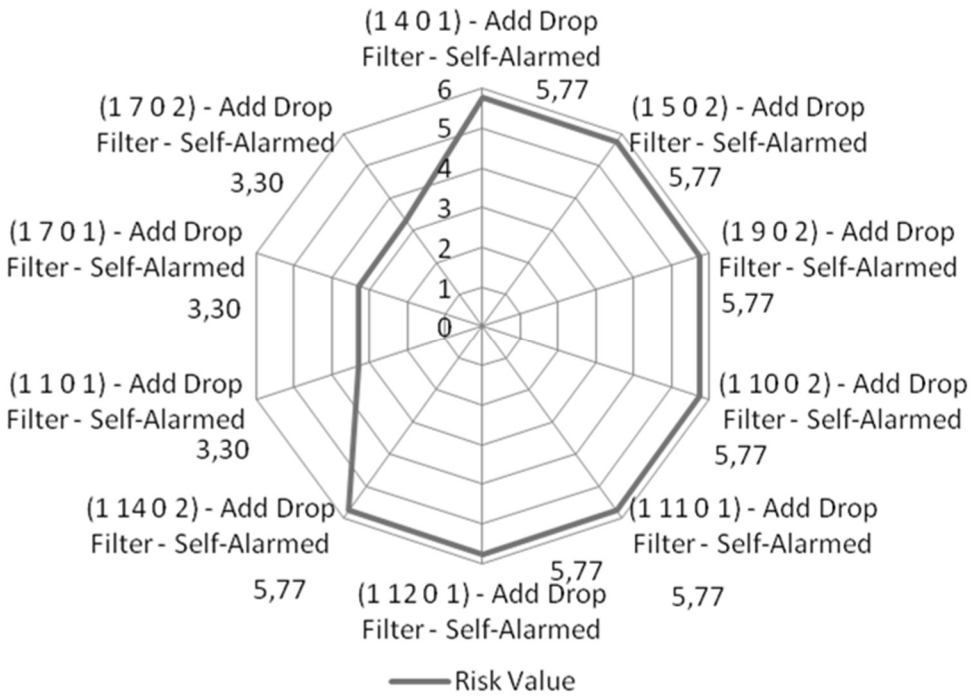


Figura 65. Riscos relacionados a categoria de elemento ADF no cenário NFSNet. Elaborado pelo autor através do ASP.

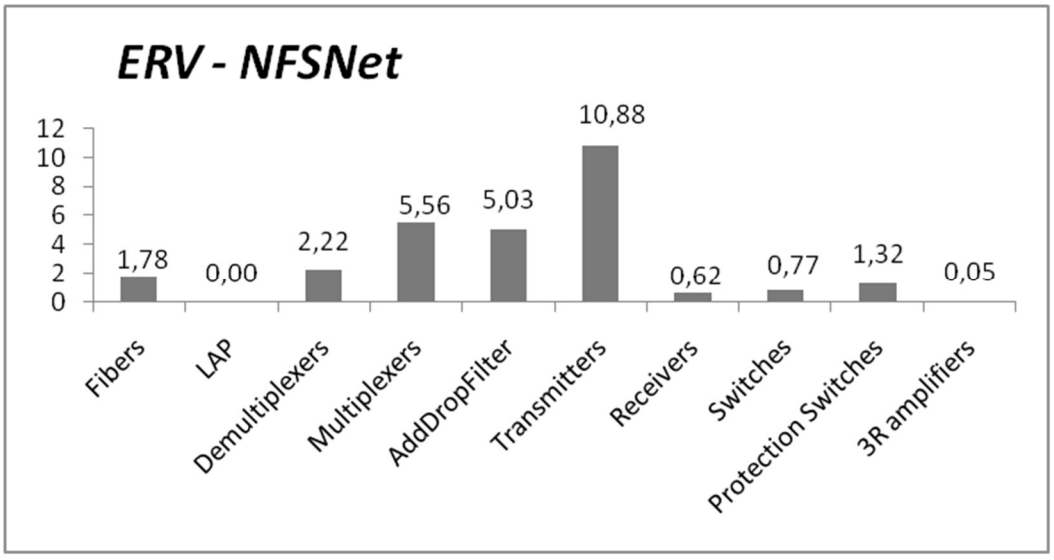


Figura 66. Riscos estimados por categoria de elemento. Segundo cenário. Elaborado pelo autor através do ASP.

A Figura 67 mostra o risco estimado para a categoria de elemento *Fiber*, para cenário *NFSNet*. Se comparado ao cenário *ARPA2NET*, pode-se observar que a categoria *Fiber* apresentou uma menor dispersão de valor de risco nesse cenário.

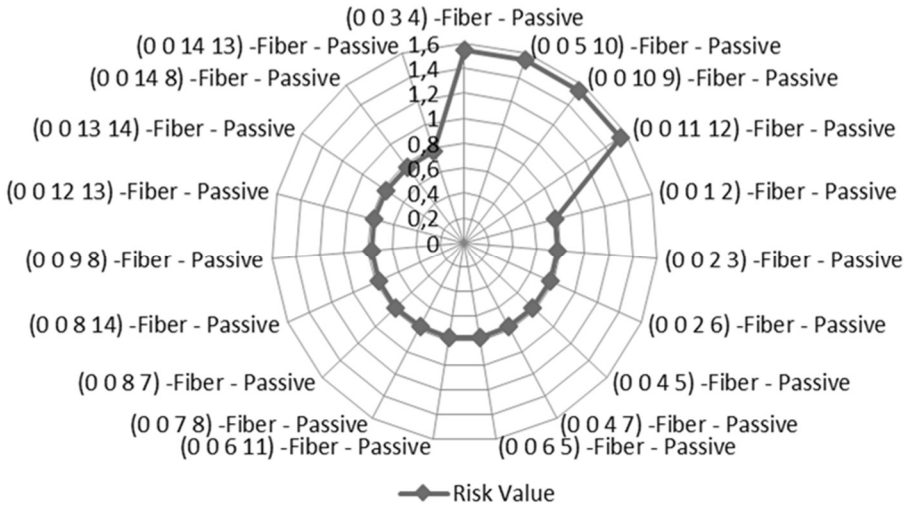


Figura 67. Riscos relacionados a categoria de elemento *Fiber* no cenário NFSNet. Elaborado pelo autor através do ASP.

Os resultados da validação estatística da simulação realizada para o cenário *NFSNET* são apresentados pelo *software* ASP (Vide Figura 68), possibilitando aos gestores verificar a assertividade e consistência da simulação realizada, através da avaliação moda, desvio-padrão, média, mediana, valor mínimo e valor máximo.

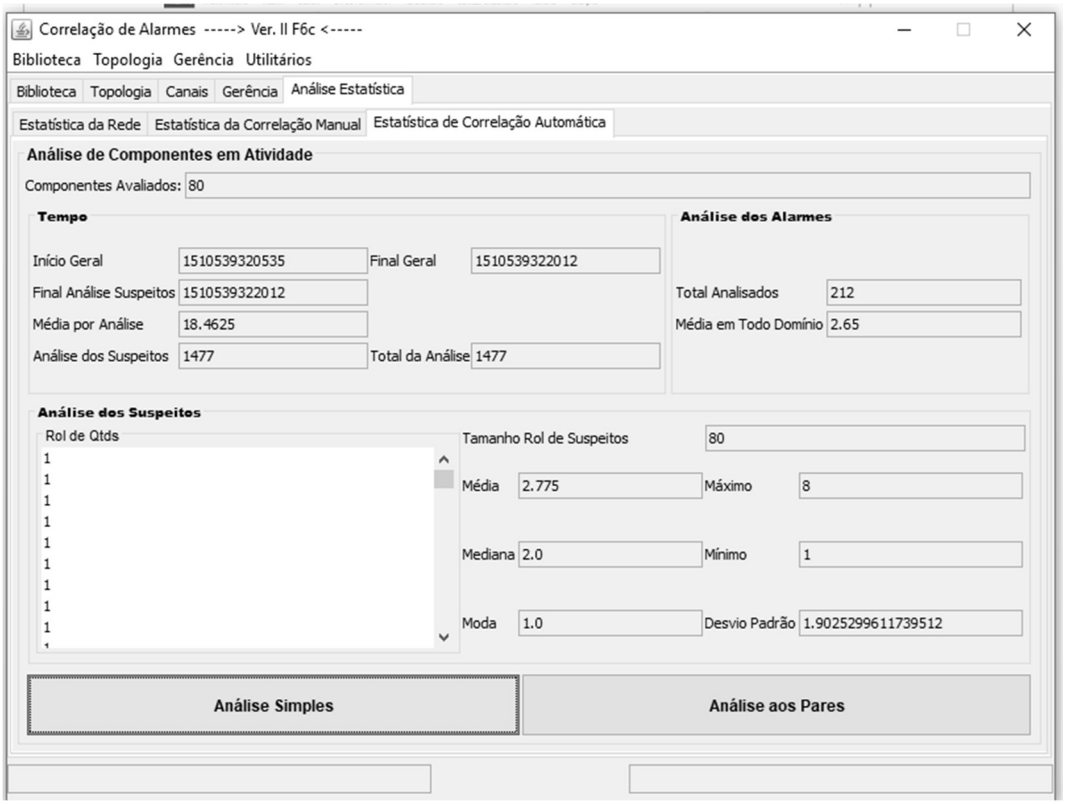


Figura 68. Tela do software *ASP* mostrando dados de validação estatística da simulação da rede *NFSnet*. Elaborado pelo autor através do ASP.

5.2.1.3 Apresentação e discussão dos resultados do Cenário #3

O terceiro cenário de simulação considera uma rede de tipo *Cost239* (Figura 69-a). Sua composição inclui 11 nós, onde 7 deles são locais e os outros 4 são nós centrais. Existem 15 links e 65 elementos de rede.

Os resultados da simulação mostrados na Figura 69-b indicam que, embora um *Multiplexador* ainda seja o elemento de maior valor de risco, existem diferentes valores de risco associados aos elementos de rede do *Multiplexador* e o risco relacionado à categoria *Multiplexador* não é o valor de categoria mais alto (vide Figura 71).

Os resultados da simulação do modelo ASP para a rede Cost239, indicaram que o *Regenerator 3R (amplificadores 3R)* eram os elementos com os valores de risco mais baixos.

A Figura 70 mostra o risco relacionado à categoria de elemento de rede ADF no cenário *Cost239*. Os resultados da simulação indicaram que existem ADF com diferentes valores de risco na topologia da rede. Os gestores podem avaliar topologia, canais e distribuição de nós para identificar possíveis fontes de alarmes, que poderiam ter influenciado cada estimativa de

risco de elemento. Mesmo que houvesse um número menor de nós na rede, o elemento *ADF* apresentaria valores de risco diferentes do que os valores apresentados nos demais cenários simulados.

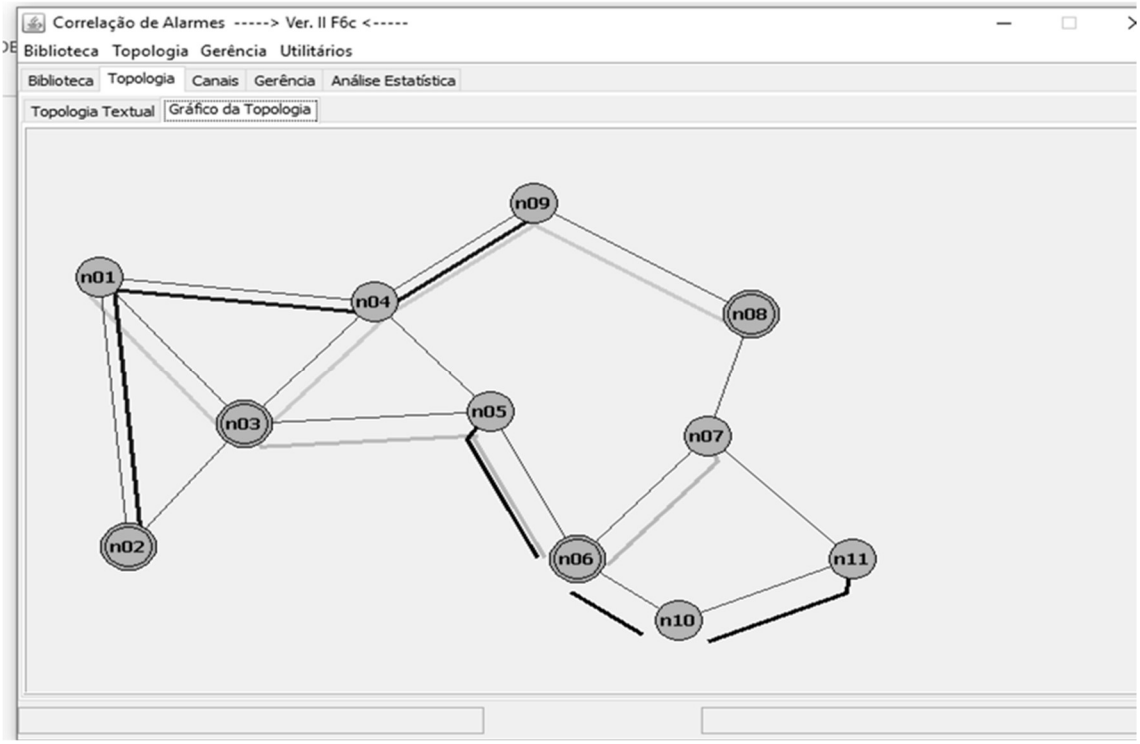


Figura 69-a. Topologia do cenário *Coast239.* Elaborado pelo autor através do ASP.

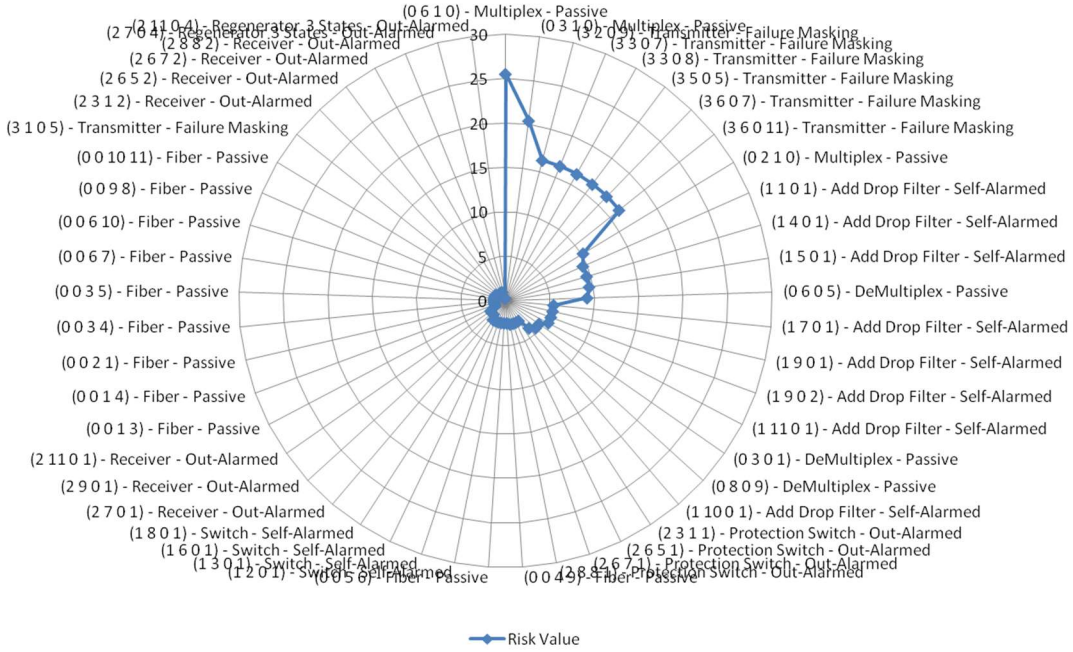


Figura 69-b. Cost239 - Zona de Risco dos elementos de rede. Elaborado pelo autor através do ASP.

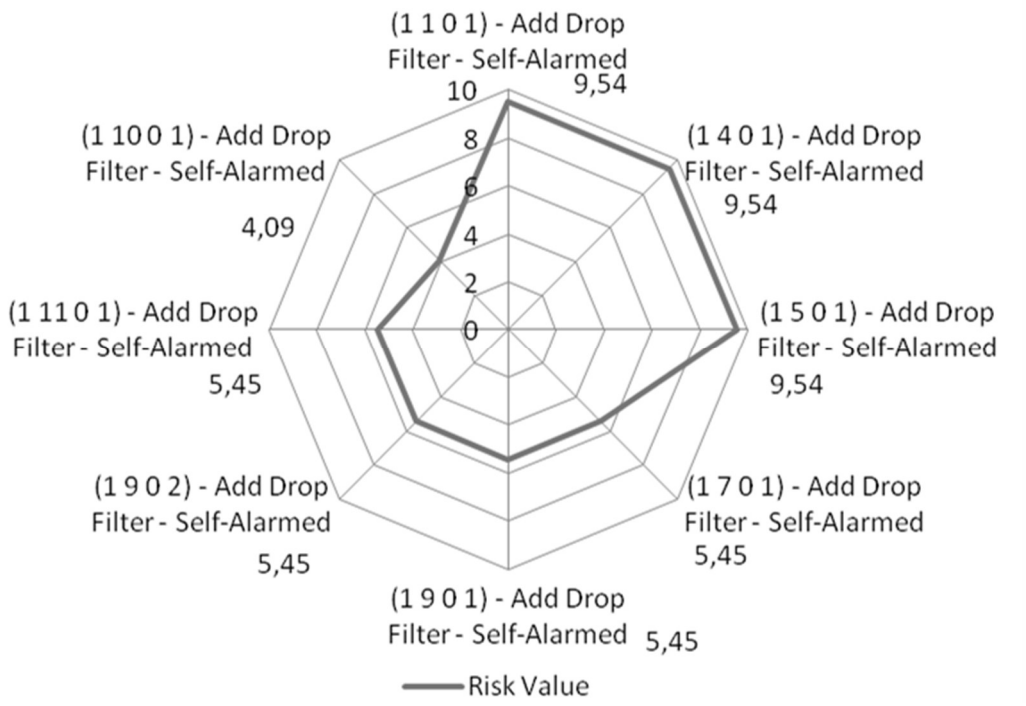


Figura 70. Risco relacionado a categoria de elemento ADF no cenário Cost239. Elaborado pelo autor através do ASP.

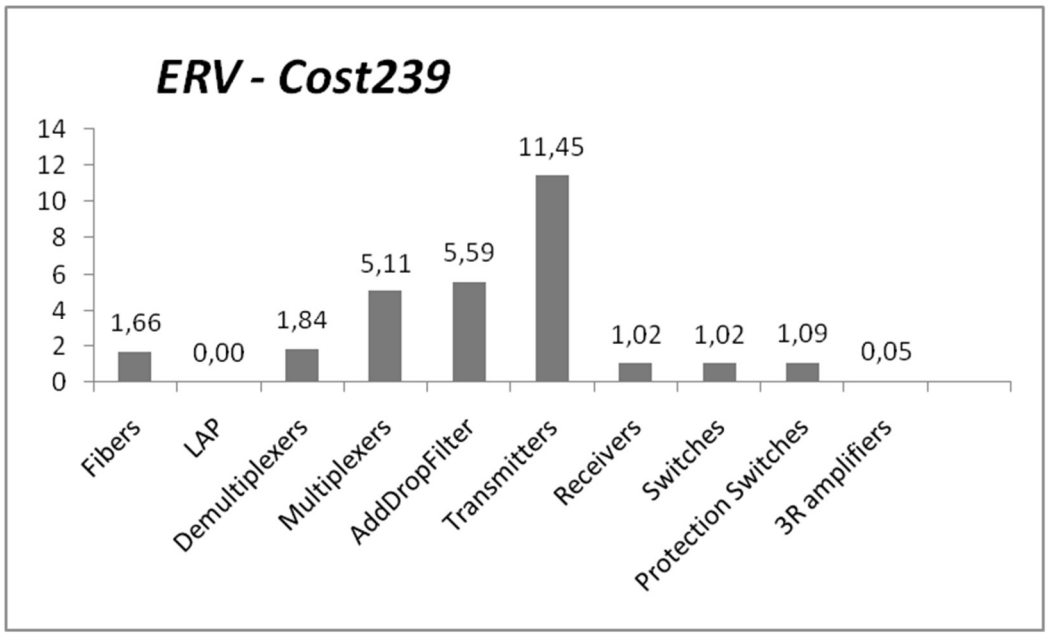


Figura 71. Risco estimado por categoria de elemento de rede - Terceiro cenário. Elaborado pelo autor através do ASP.

Os resultados da validação estatística da simulação realizada para o cenário *Cost239* são apresentados pelo *software* ASP (Vide Figura 72), possibilitando aos gestores verificar a assertividade e consistência da simulação realizada, através da avaliação moda, desvio-padrão, média, mediana, valor mínimo e valor máximo.

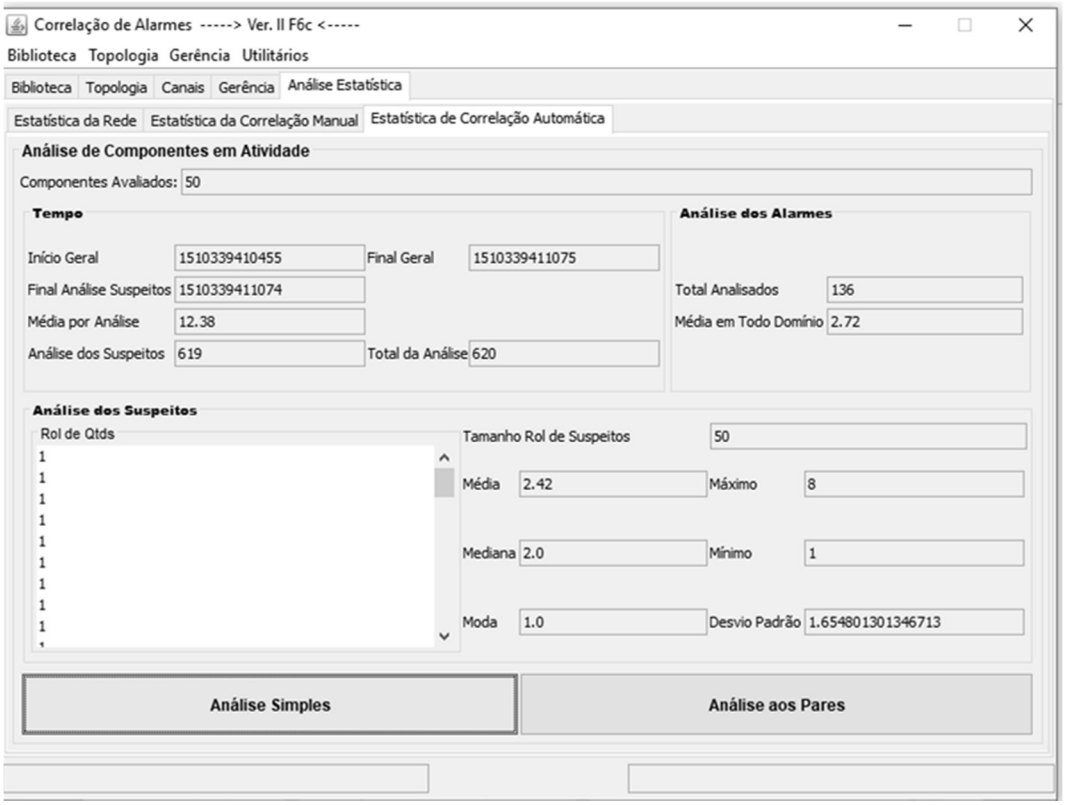


Figura 72. Tela do software *ASP* mostrando dados de validação estatística da simulação da rede *Cost239*. Elaborado pelo autor através do ASP.

5.2.1.4 Apresentação e discussão dos resultados do Cenário #4

O cenário de simulação considera uma rede de tipo *USnation* (Figura 73). Sua composição inclui 24 nós, onde 17 deles são locais e os outros 7 são nós centrais. Existem 43 links e 133 elementos de rede.

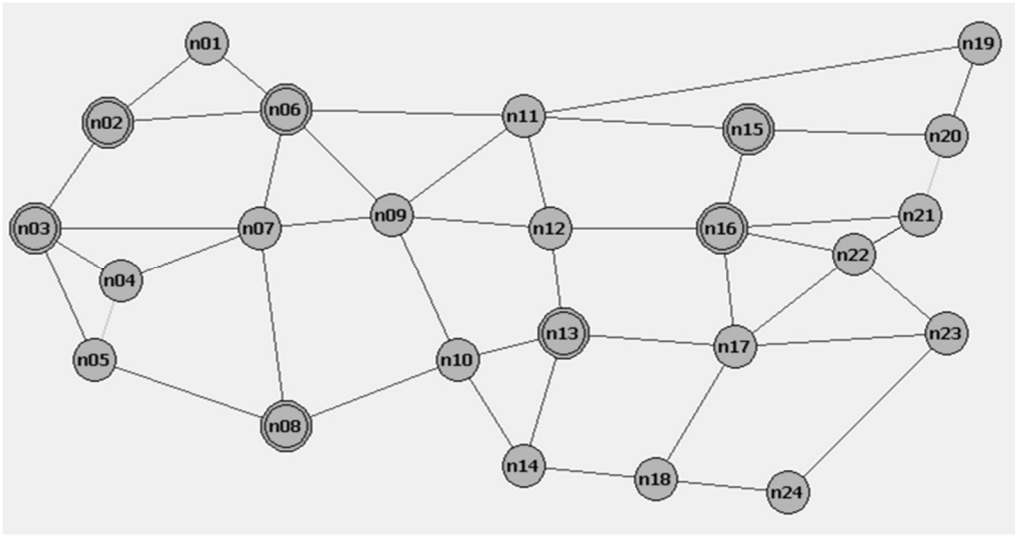


Figura 73. Topologia do cenário *USnation.* Elaborado pelo autor através do ASP.

Conforme mostrado na Figura 73, os canais passam por 17 nós locais, 7 nós centrais e 28 links. A rede *USnation* possui os seguintes parâmetros: 28 fibras, que geram 96 alarmes; 7 LAP, que não geram alarmes; 7 Demultiplexadores, que geram 24 alarmes; 7 Multiplexadores, que geram 27 alarmes; 19 Add / Drop Filter (ADFs), que geram 103 alarmes; 13 transmissores, que geram 52 alarmes; 13 receptores, que geram 18 alarmes; 7 switches, que geram 7 alarmes; 13 Interruptores de proteção, que geram 16 alarmes e 13 amplificadores 3R, que geram 5 alarmes. Existe um total de 127 componentes de rede usados e 348 alarmes gerados. Os valores das probabilidades de falhas estimadas para os elementos de rede no estudo de caso são mostrados na Figura 3. Conforme mencionado anteriormente, no modelo *ASP*, cada elemento de probabilidade de falha é estimado pelos gestores.

Procedeu-se a simulação do cenário *USnation* por meio da ferramenta de software ASP (Figura 74).

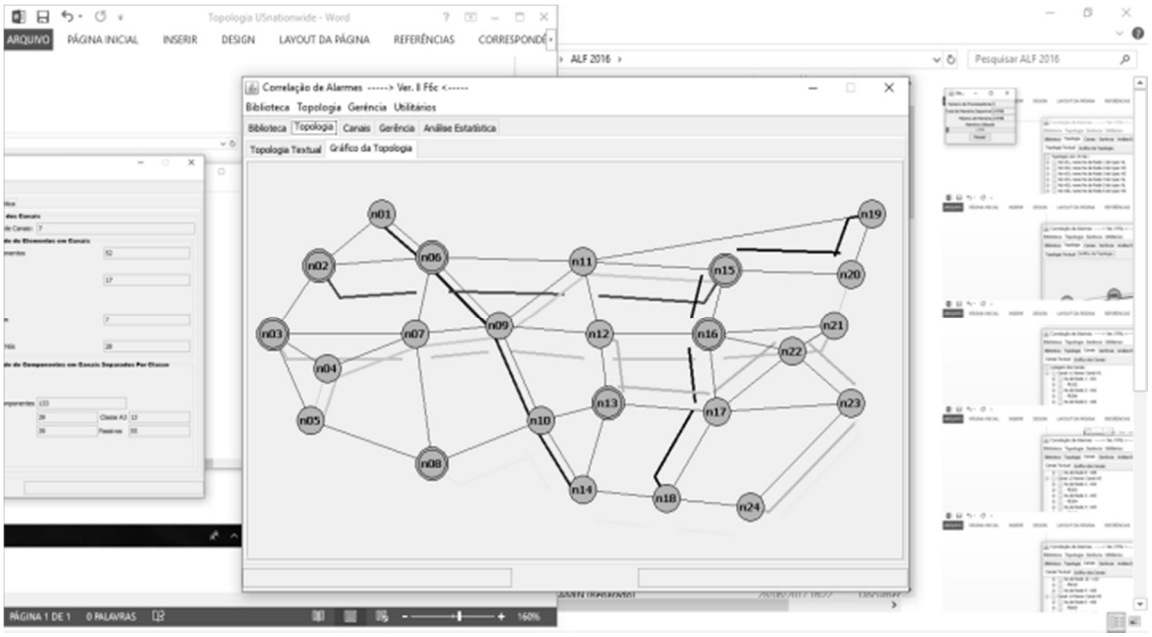


Figura 74. Simulação do cenário *USnation* no *software ASP*. Elaborado pelo autor através do ASP.

O modelo ASP gera uma tabela de classificação de risco que inclui todos os elementos da rede óptica do cenário. A Tabela 9 mostra os riscos dos primeiros 24 elementos da rede. A Figura 75 mostra a zona de risco dos elementos de rede Usnation. Um Multiplexador é o elemento com maior risco. Os gerentes podem analisar intervalos de risco e proceder a uma análise aprofundada usando esta informação, para decidir sobre a escolha de pontos de redundância. Os gerentes da empresa Alpha citaram que esse suporte melhora a qualidade de decisão. Os resultados da simulação do modelo ASP para a rede USnation, indicaram que o Regenerator 3R (amplificadores 3R) eram os elementos com valores de risco mais baixos.

A Tabela 4 mostra os primeiros 24 elementos na classificação de risco gerada pelo modelo *ASP*. Os valores de risco (*ERVs*), estimados pelo modelo *ASP* são influenciados pela topologia de rede, canais e impacto comercial. Pode-se observar que o risco relacionado aos Multiplexadores, Transmissores e ADFs está em diferentes posições no ranking, devido a possíveis diferenças em sua localização na topologia, aos canais e em função de sua relevância para o negócio.

Tabela 9. Ranking de risco com os 24 primeiros elementos para o cenário USnation. Elaborado pelo autor.

Network Element	Risk Value
(0 6 1 0) - Multiplexer - Passive	9,10
(0 16 1 0) - Multiplexer - Passive	9,10
(3 1 0 5) - Transmitter - Failure Masking	7,28
(3 2 0 15) - Transmitter - Failure Masking	7,28
(3 3 0 21) - Transmitter - Failure Masking	7,28
(3 5 0 6) - Transmitter - Failure Masking	7,28
(3 6 0 14) - Transmitter - Failure Masking	7,28
(3 6 0 15) - Transmitter - Failure Masking	7,28
(3 8 0 23) - Transmitter - Failure Masking	7,28
(3 13 0 12) - Transmitter - Failure Masking	7,28
(3 15 0 18) - Transmitter - Failure Masking	7,28
(3 16 0 18) - Transmitter - Failure Masking	7,28
(3 16 0 21) - Transmitter - Failure Masking	7,28
(3 19 0 5) - Transmitter - Failure Masking	7,28
(3 24 0 6) - Transmitter - Failure Masking	7,28
(1 9 0 1) - Add Drop Filter - Self Alarmed	6,07
(0 2 1 0) - Multiplexer - Passive	4,55
(0 3 1 0) - Multiplexer - Passive	4,55
(0 8 1 0) - Multiplexer - Passive	4,55
(0 13 1 0) - Multiplexer - Passive	4,55
(0 15 1 0) - Multiplexer - Passive	4,55
(1 7 0 1) - Add Drop Filter - Self Alarmed	4,25
(1 10 0 1) - Add Drop Filter - Self Alarmed	4,25
(1 11 0 1) - Add Drop Filter - Self Alarmed	4,25

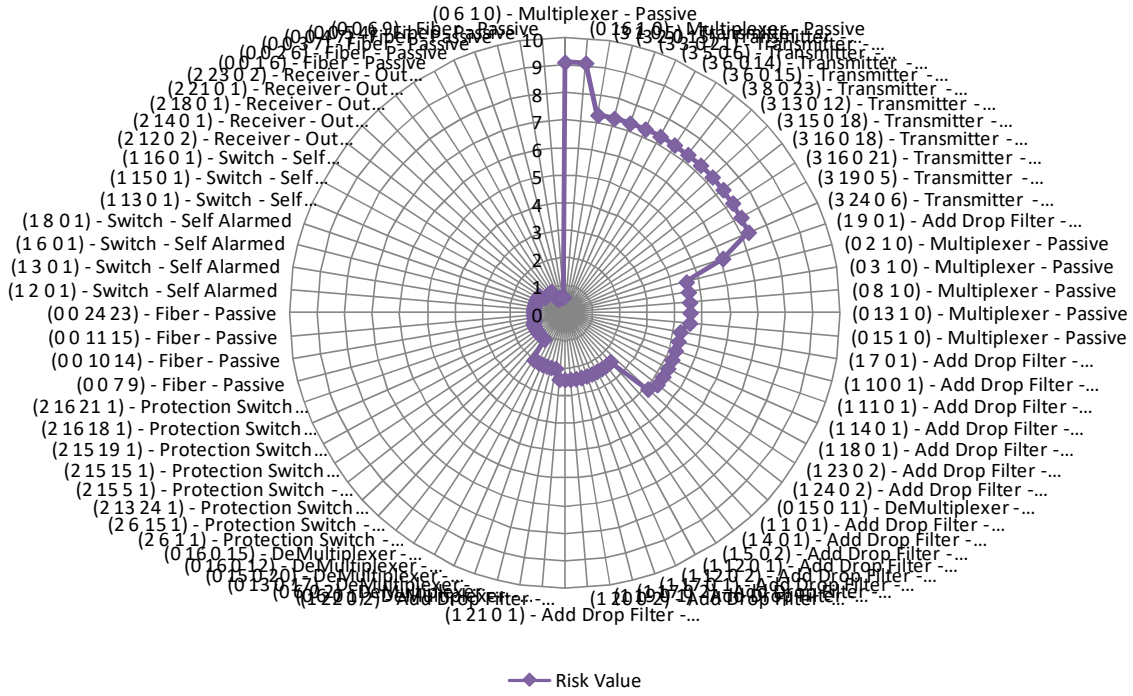


Figura 75. Zona de riscos do cenário *USnation.* Elaborado pelo autor através do ASP.

Na Figura 76, pode-se observar que o risco (*ERV*) para cada elemento de rede foi estimado em uma zona de risco entre 4,5 e 9,1. O Multiplexador localizado na notação de topologia (0 6 1 0) possui o maior valor de risco e provavelmente receberá redundância. Todos os níveis de prioridade de elementos são mostrados e esta decisão de redundância é suportada pelo modelo *ASP*.

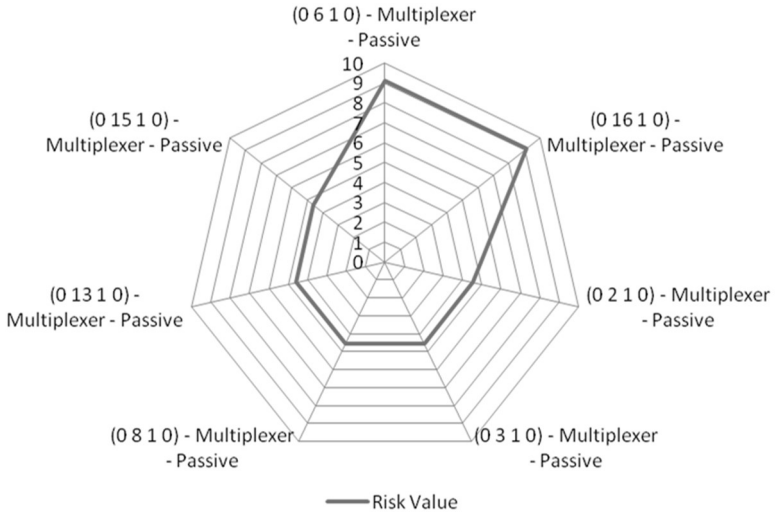


Figura 76. Riscos relacionados à categoria de elemento Multiplexador - cenário *USnation.* Elaborado pelo autor através do ASP.

A Figura 77 mostra o risco relacionado à categoria de elemento de rede ADF no cenário da Nação dos EUA. Os resultados da simulação indicaram que o modelo *ASP* identificou *ADFs* com diferentes valores de risco na topologia da rede. Os gerentes podem avaliar topologia, canais e distribuição de nós para identificar possíveis fontes de alarmes, que poderiam ter influenciado cada estimativa de risco de elemento.

A zona de risco dos elementos da categoria ADFs (intervalo entre 2,4 e 6) pode mostrar 11 ADFs com valor de risco 2,4 e 8 ADFs com valor de risco maior. Os gerentes podem analisar esta informação e a localização dos nós ADF para ajudar no processo de tomada de decisão. Outra informação útil que pode ser gerada pelo modelo *ASP* para os gestores é o valor de risco relacionado a cada categoria de elemento, como suporte complementar à tomada de decisão.

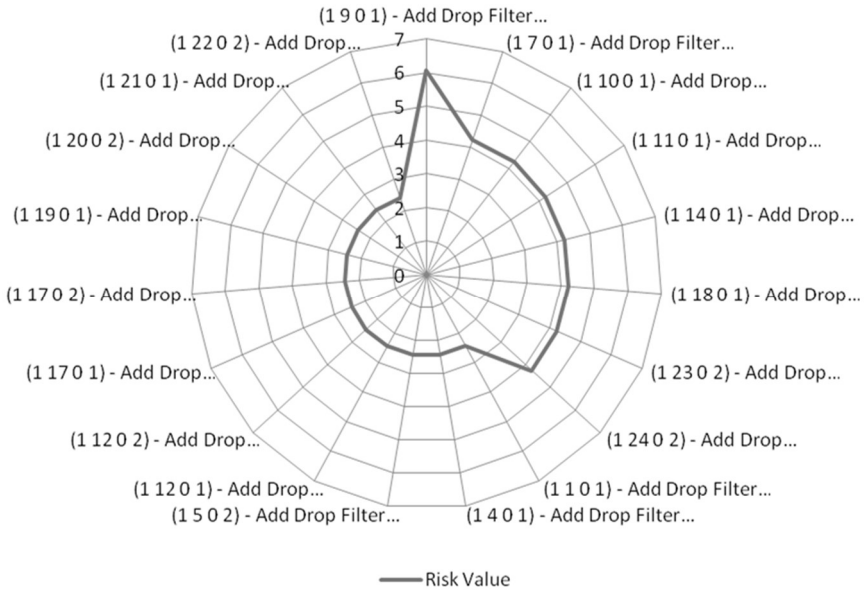


Figura 77. Riscos relacionados à categoria de elemento ADF - cenário *USnation.* Elaborado pelo autor através do ASP.

A zona de risco dos elementos da categoria *Fibra* está localizada no intervalo entre 0,57 e 1,14 (vide Figura 78). Os elementos com maior valor de risco identificados foram: (0 0 7 9), (0 0 10 14), (0 0 11 15) e (0 0 24 23).

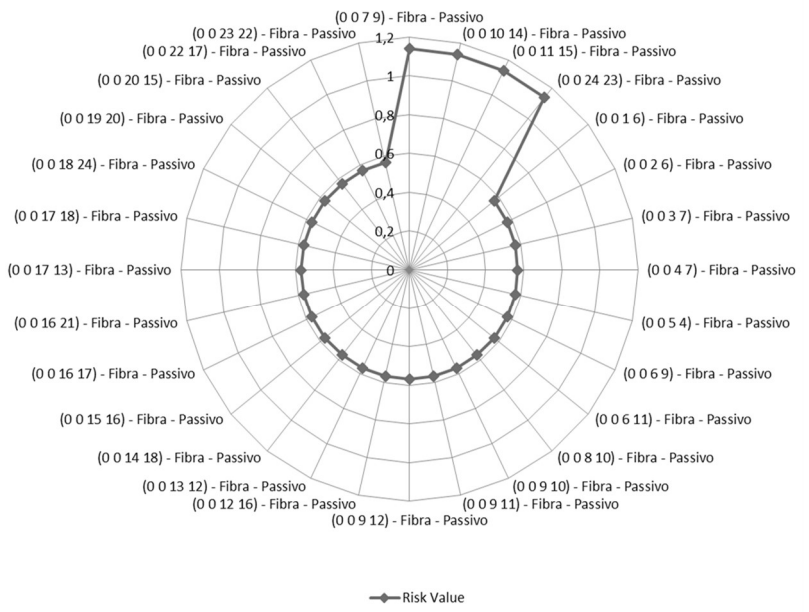


Figura 78. Riscos relacionados à categoria de elemento Fibra - cenário *USnation.* Elaborado pelo autor através do ASP.

A zona de risco dos elementos da categoria *Receptor* está localizada no intervalo entre 0,46 e 0,91 (vide Figura 79). Os elementos com maior valor de risco identificados foram: (21202), (21401), (21801), (22101) e (2 23 0 2).

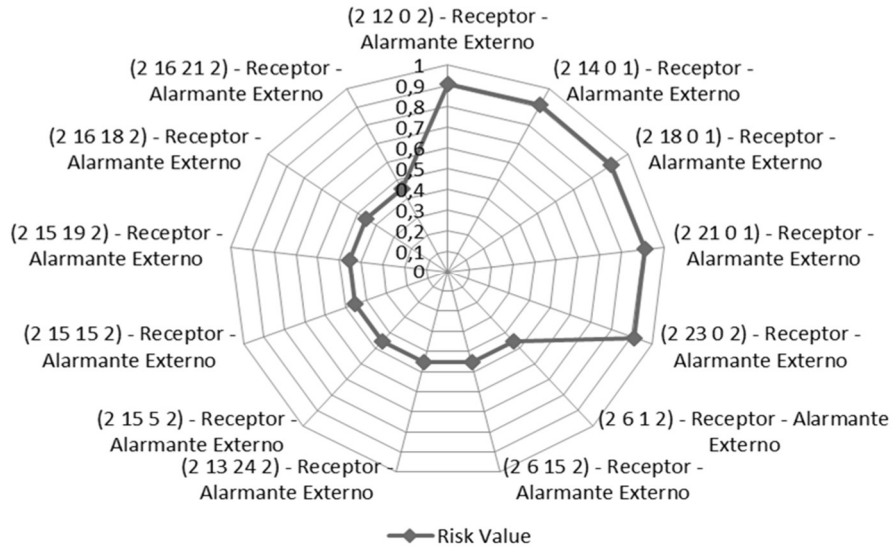


Figura 79. Riscos relacionados à categoria de elemento Receptor - cenário *USnation.* Elaborado pelo autor através do ASP.

Os resultados da validação estatística da simulação realizada para o cenário *USnation* são apresentados pelo *software* ASP (Vide Figura 80), possibilitando aos gestores verificar a assertividade e consistência da simulação realizada, através da avaliação moda, desvio-padrão, média, mediana, valor mínimo e valor máximo.

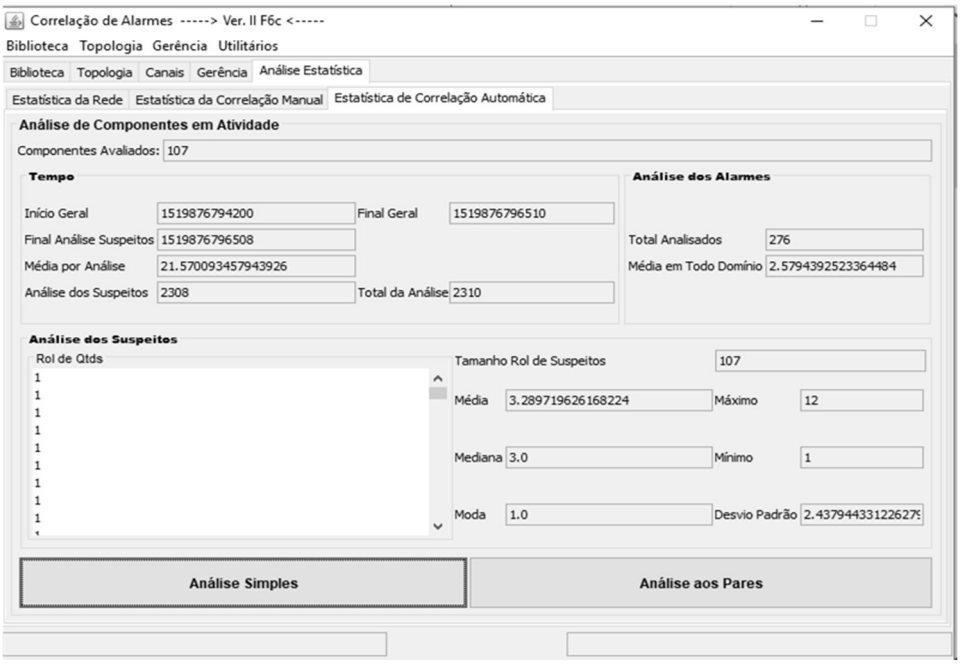


Figura 80. Tela do software *ASP* mostrando dados de validação estatística da simulação da rede *USnation*. Elaborado pelo autor através do ASP.

5.2.1.5 Apresentação e discussão dos resultados do Cenário #5

O quinto cenário de simulação considera uma rede de tipo *ER_NET* (Figura 81). Sua composição inclui 37 nós, onde 24 deles são locais e os outros 13 são nós centrais. Existem 65 links e 128 elementos de rede.

Conforme mostrado na Figura 81, os canais passam por 24 nós locais, 13 nós centrais e 65 links. A rede *ER_NET* possui os parâmetros já mostrados na Tabela 3.

Os valores das probabilidades de falhas estimadas para os elementos de rede no estudo de caso são mostrados na Figura 44. Conforme mencionado anteriormente, no modelo *ASP*, cada elemento de probabilidade de falha é estimado pelos gestores. Durante os testes referentes ao cenário ER_NET, foram avaliadas as duas fórmulas de cálculo para o impacto de um elemento de rede (Expressões de 1 a 4) nas simulações.

Procedeu-se a simulação do cenário *ER_NET* por meio da ferramenta de software ASP (Figura 82).

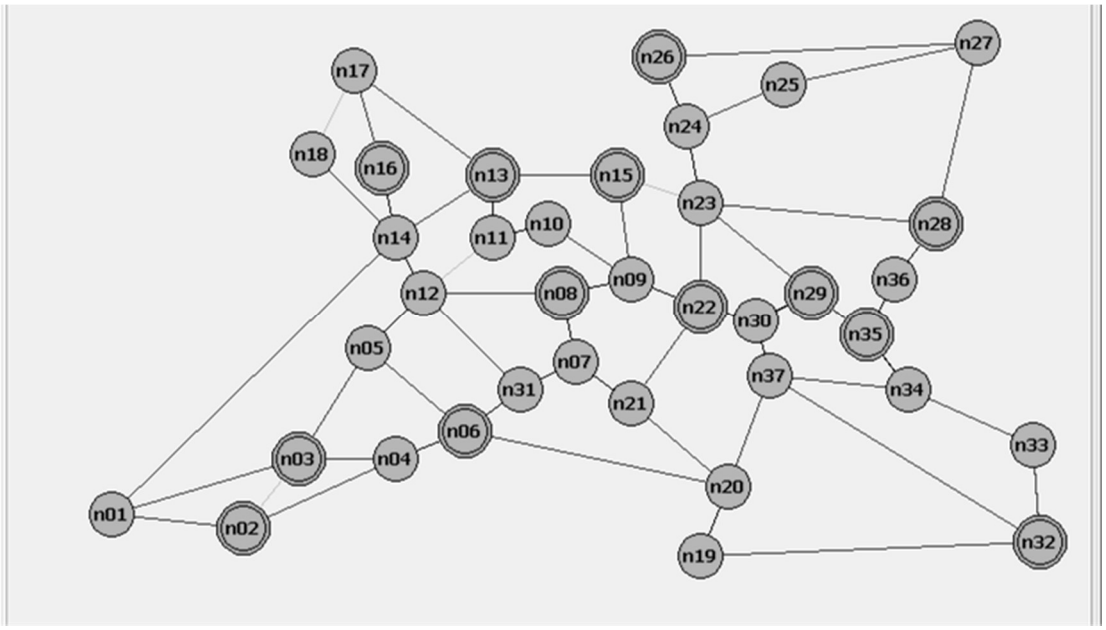


Figura 81. Topologia do cenário *ER_NET*. Elaborado pelo autor através do ASP.

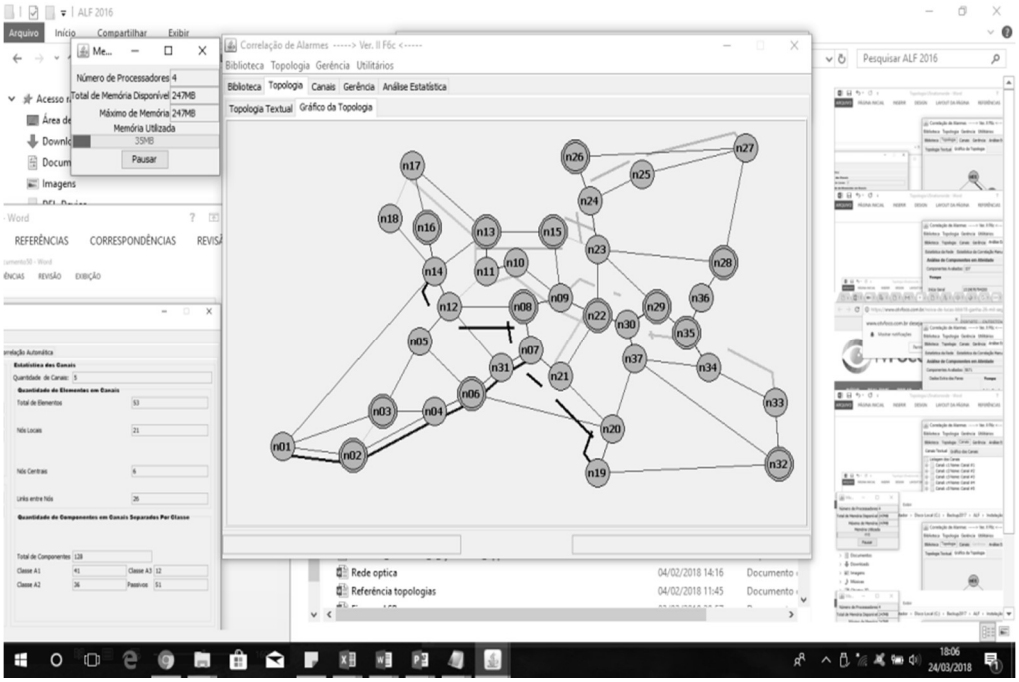


Figura 82. Simulação do cenário *ER_NET* no *software ASP*. Elaborado pelo autor através do ASP.

Na Figura 83, pode-se observar que o risco (*ERV*) para cada elemento de rede foi estimado em uma zona de risco entre 0,5 e 10,2. O Multiplexador localizado na notação de topologia (0 22 1 0) possui o maior valor de risco e provavelmente receberá redundância. Todos os níveis de prioridade de elementos são mostrados e esta decisão de redundância é suportada pelo modelo *ASP*. Os elementos de rede com o menor risco identificado pertencem às categorias Regeneradores e Receptores. A qualquer momento, os gestores podem acessar a lista completa com o *ranking* gerado pelo *ASP*, caso necessitem avaliar a localização de cada elemento, para uma possível tomada de decisão.

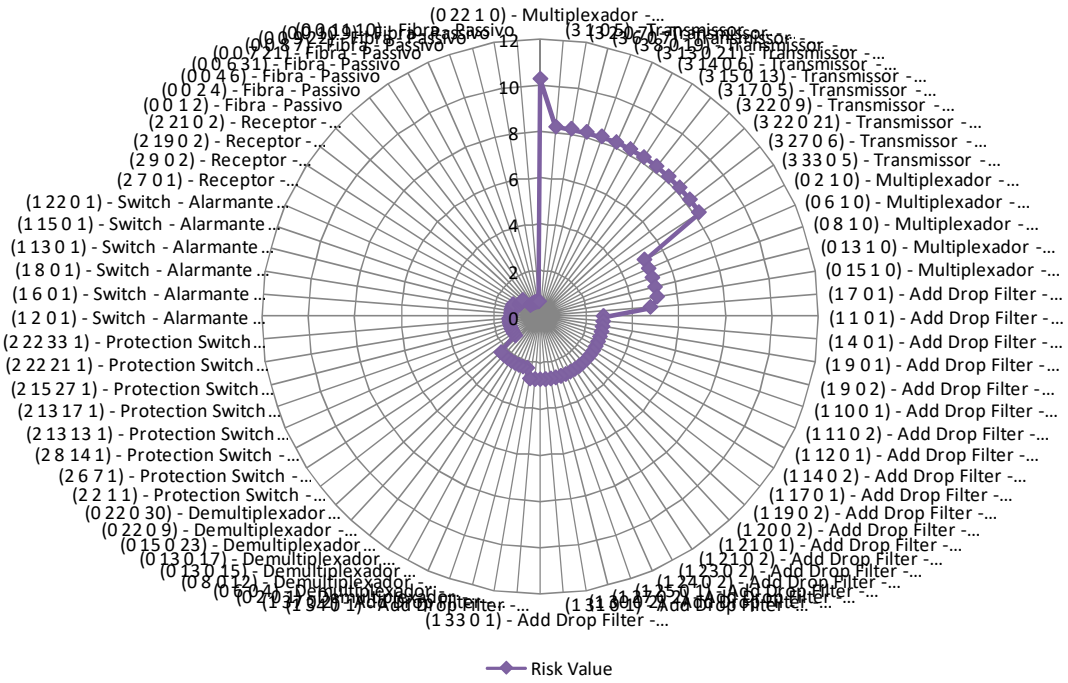


Figura 83. Zona de riscos do cenário *ER_NET - Impacto Simplificado.* Elaborado pelo autor através do ASP.

A Tabela 10 mostra os primeiros 24 elementos na classificação de risco gerada pelo modelo *ASP*. Como citado anteriormente, os valores de risco (*ERVs*) para os elementos da rede são estimados pelo modelo *ASP*, influenciados pela topologia de rede, canais e impacto para o negócio. Pode-se observar que o risco relacionado aos Multiplexadores, Transmissores e ADFs encontra-se distribuído em diferentes posições no *ranking*, provavelmente por conta de possíveis diferenças em sua localização na topologia, quantidade de canais que passam pelo mesmo, além do grau de sua relevância para o negócio.

Tabela 10. Ranking de risco com os 24 primeiros elementos para o cenário ER_NET

Network Element	Risk Value
(0 22 1 0) - Multiplexador - Passivo	10,28
(3 1 0 5) - Transmissor - Mascarador	8,23
(3 2 0 7) - Transmissor - Mascarador	8,23
(3 6 0 7) - Transmissor - Mascarador	8,23
(3 8 0 19) - Transmissor - Mascarador	8,23
(3 13 0 21) - Transmissor - Mascarador	8,23
(3 14 0 6) - Transmissor - Mascarador	8,23
(3 15 0 13) - Transmissor - Mascarador	8,23
(3 17 0 5) - Transmissor - Mascarador	8,23
(3 22 0 9) - Transmissor - Mascarador	8,23

(3 22 0 21) - Transmissor - Mascarador	8,23
(3 27 0 6) - Transmissor - Mascarador	8,23
(3 33 0 5) - Transmissor - Mascarador	8,23
(0 2 1 0) - Multiplexador - Passivo	5,14
(0 6 1 0) - Multiplexador - Passivo	5,14
(0 8 1 0) - Multiplexador - Passivo	5,14
(0 13 1 0) - Multiplexador - Passivo	5,14
(0 15 1 0) - Multiplexador - Passivo	5,14
(1 7 0 1) - Add Drop Filter - Alarmante Interno	4,80
(1 1 0 1) - Add Drop Filter - Alarmante Interno	2,74
(1 4 0 1) - Add Drop Filter - Alarmante Interno	2,74
(1 9 0 1) - Add Drop Filter - Alarmante Interno	2,74
(1 9 0 2) - Add Drop Filter - Alarmante Interno	2,74
(1 10 0 1) - Add Drop Filter - Alarmante Interno	2,74

Conforme pode ser identificado a partir da Figura 84, a segunda simulação do cenário *ER_NET* sinalizou uma mudança radical na zona de risco, em função da utilização da segunda fórmula proposta nesta Tese, para o cálculo do impacto de um elemento de rede. A partir da utilização de dados da rede óptica da empresa *Alpha* como base da estimativa do tempo médio entre falhas e tempo médio de reparo para cada categoria de elemento de rede na simulação, nota-se que os elementos da categoria Fibra passaram a ocupar o topo no *ranking* de risco gerado pelo modelo *ASP*, por conta das estatísticas da empresa indicarem que existem rupturas na Fibra a cada 3,5 dias, demandando muitas ações de reparo na topologia, fator que associado a sua relevância para o negócio e quantidade de alarmes identificados na simulação, geraram esse novo indicativo, que foi considerado muito útil pelos gestores. Planeja-se a criação de uma biblioteca de possíveis equações para cálculo do impacto de um elemento de rede óptica em trabalhos futuros. Essa biblioteca permitirá a comparação dos resultados de uma série de avaliações de impacto (*Business Impact Analysis - BIA*), ajudando os gestores no processo de tomada de decisão relativo à escolha de pontos passíveis de redundância no cenário de rede óptica simulado.

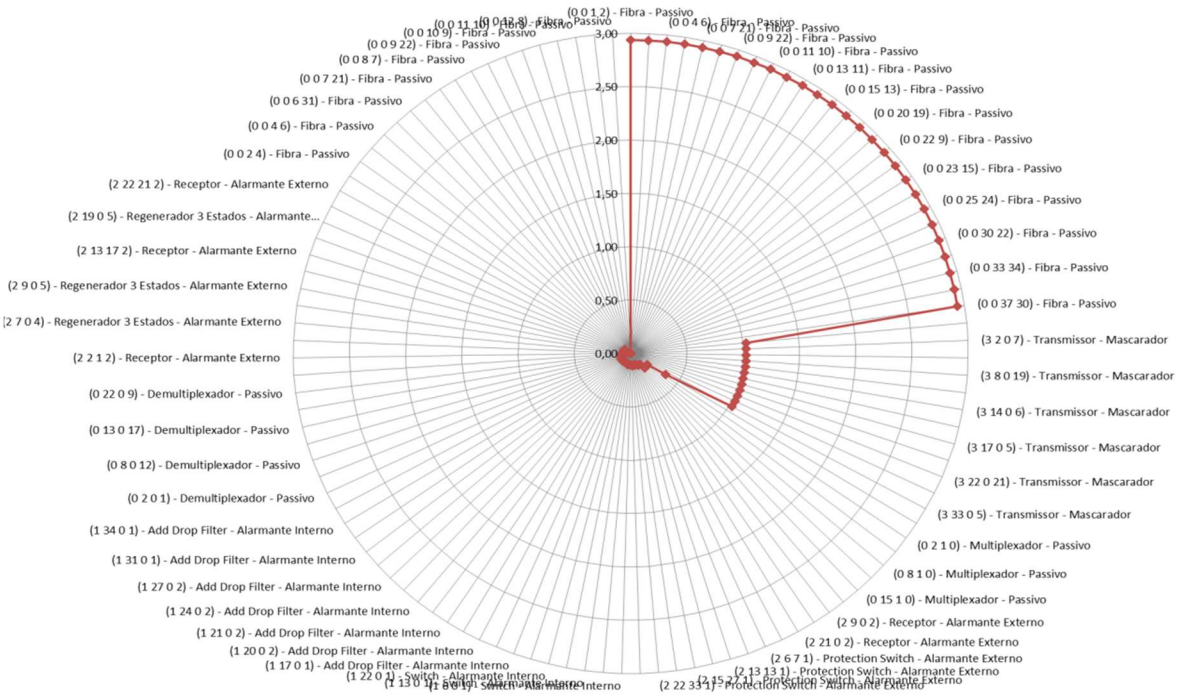


Figura 84. Zona de riscos do cenário *ER_NET - Considerando o cálculo do Impacto de Reparo.* Elaborado pelo autor através do ASP.

O Multiplexador do nó 22 apresentou o maior valor de risco em relação aos demais multiplexadores, pelo fato da existência de um maior número de canais passando pelo mesmo, o que pode concatenar uma maior quantidade de alarmes no caso de uma falha (Figura 85).

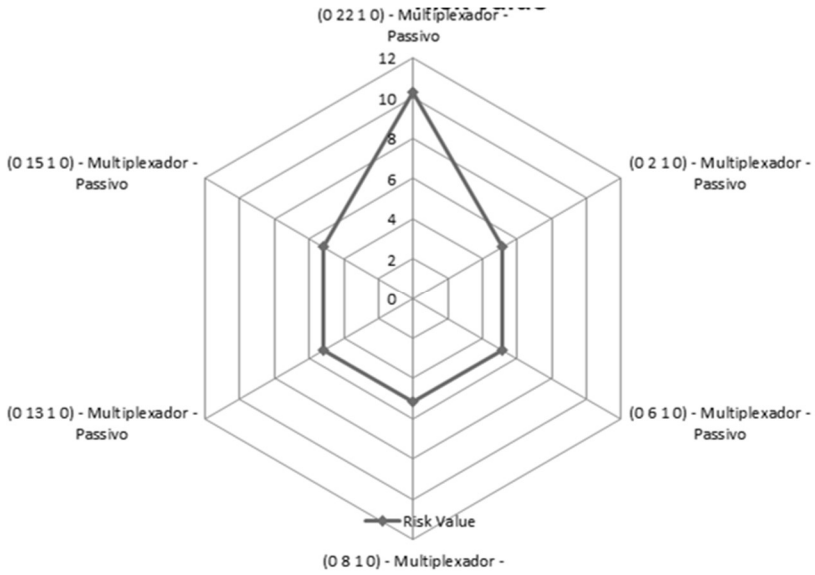


Figura 85. Riscos relacionados à categoria de elemento Multiplexador - cenário *ER_NET - Impacto Simplificado.* Elaborado pelo autor através do ASP.

Ao se comparar os resultados das simulações do cenário *ER_NET* com impacto simplificado e a que considerou o impacto do reparo (Figuras 86 e 87), pode-se notar que houve apenas uma variação de resultados para o elemento de rede da categoria *Receptor*, por conta da inclusão do impacto de reparo no cálculo do impacto para o negócio. Entretanto, alguns elementos da topologia podem ter mudado de posição no *ranking* geral de risco calculado pelo modelo *ASP*. A mesma inferência se aplica para os demais elementos de rede da topologia avaliada nas duas simulações.

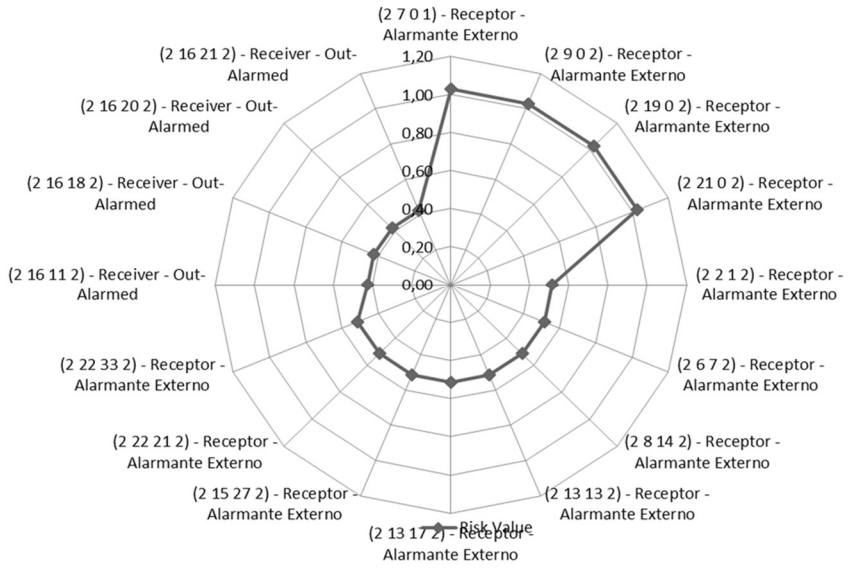


Figura 86. Riscos relacionados à categoria de elemento Receptor - cenário *ER_NET - Impacto simplificado.* Elaborado pelo autor através do ASP.

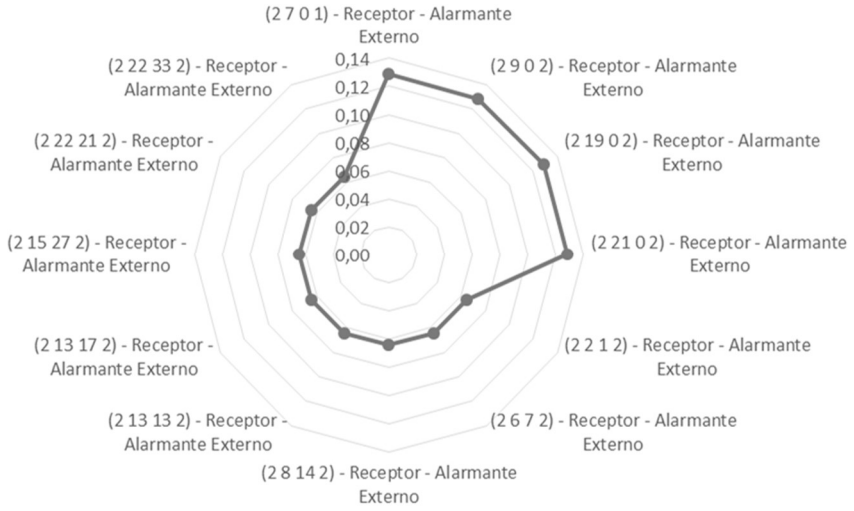


Figura 87. Riscos relacionados à categoria de elemento Receptor - cenário *ER_NET - Considerando o cálculo do impacto de Reparo.* Elaborado pelo autor através do ASP.

Os resultados da validação estatística de cada simulação são apresentados pelo *software ASP*, possibilitando aos gestores verificar a assertividade e consistência da simulação realizada, através da moda, desvio-padrão, média, mediana, valor mínimo e valor máximo (Figura 88).

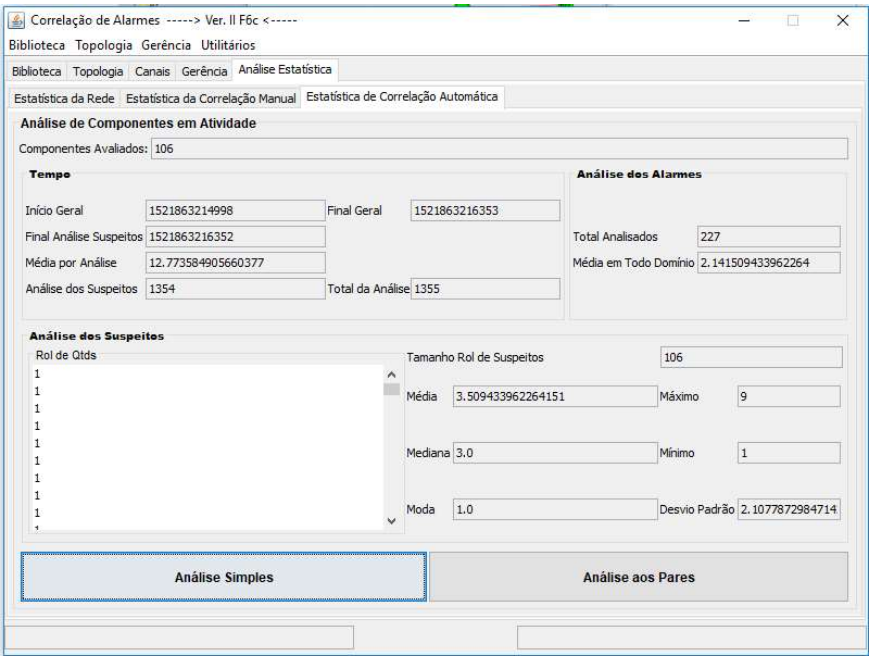


Figura 88. Tela do software *ASP* mostrando dados de validação estatística da simulação da rede *ER_NET*. Elaborado pelo autor através do ASP.

Na primeira fase da pesquisa, de caráter exploratório, foi identificada uma organização que administra redes ópticas. Foram realizadas entrevistas e pesquisa documental visando aquisição de conhecimento sobre o gerenciamento de serviços, incidentes, problemas e falhas de redes ópticas na organização pesquisada. Gestores de TI e de Redes foram entrevistados sobre os temas: alinhamento estratégico TI/negócios, tomada de decisão no gerenciamento falhas e verificação de benefícios do serviço de rede. Observou-se na organização avaliada um alto uso de práticas de gerenciamento de falhas, sem a devida análise dos benefícios e dos riscos envolvidos, bem como sem o alinhamento desta iniciativa com os objetivos organizacionais.

Paralelamente, foi realizada revisão bibliográfica na literatura, para um aprofundamento teórico sobre o problema identificado. Definiu-se que o simulador a ser desenvolvido teria o seguinte foco de análise: identificar pontos críticos passíveis de redundância em redes ópticas, com base no risco para o negócio. A partir das entrevistas realizadas na fase inicial e da análise dos dados empíricos levantados na organização pesquisada, foi possível a identificação de

padrões de comportamento conhecidos, comportamentos problemáticos, relações causais e equações de interesse.

Os testes de sensibilidade dos parâmetros de entrada e de calibragem do modelo proposto foram executados em três momentos distintos: a) durante a execução dos testes estruturais, com o objetivo de corrigir equações; b) durante os testes de comportamento, com o objetivo de eliminar parâmetros e procedimentos de pouca relevância e calibrar corretamente o modelo e; c) durante a execução de testes de aprendizado, com o objetivo de gerar incerteza nas entradas e analisar riscos. Os resultados obtidos com os testes subsidiaram o refinamento do modelo.

A fase final desta pesquisa consistiu na utilização, manutenção e avaliação da efetividade do modelo para a análise de falhas em uma visão de negócio. Sessões de utilização do modelo foram realizadas com os gestores da organização pesquisada. Através de cenários, foi possível proceder simulações e avaliar o modelo em 5 cenários distintos de redes ópticas de referência. A atividade final de validação de aprendizagem foi obter a avaliação dos gestores a respeito da efetividade do modelo como ferramenta de apoio a decisão. Foram usados formulários e entrevistas para este fim. Os resultados da análise quantitativa (formulários) e qualitativa (entrevistas) apontaram para a aceitação das hipóteses de pesquisa. Diante dos resultados obtidos, há indicativos de que o uso do modelo como ferramenta pode resultar em um processo mais bem sucedido de gerenciamento de falhas. Isto sustenta a tese aqui defendida, partindo do pressuposto que os objetivos do gerenciamento de falhas em redes ópticas devem estar alinhados com benefícios pretendidos para o negócio.

A impossibilidade de generalização dos resultados é uma limitação desta pesquisa. A escolha de uma amostra por conveniência, bem como o uso de dados empíricos de uma organização sinalizam para resultados que não podem ser generalizados em sua plenitude.

6 CONCLUSÃO E TRABALHOS FUTUROS

6.1 CONSIDERAÇÕES FINAIS

Este trabalho apresentou um modelo baseado em risco para auxiliar os gestores no processo de identificação de pontos críticos em redes ópticas. O modelo proposto apoia o processo de tomada de decisão nas atividades de gerenciamento de serviços, considerando o impacto de risco. O lançamento do modelo, implementado na ferramenta de software *ASP*, fornece aos gestores um *ranking* de riscos, com os quais os mesmos podem identificar de forma rápida e assertiva os pontos críticos que podem ser aplicados para estabelecer redundância em uma rede óptica.

Este modelo é diferente dos modelos relacionados, porque os gestores podem usar uma visão de negócio para identificar pontos de redundância em redes ópticas; visa auxiliar no processo de tomada de decisão em atividades de gerenciamento de falhas, considerando o impacto de risco; não é intrusivo e pode ser usado em adição às ferramentas de gerenciamento de incidentes e gerenciamento de falhas existentes.

Os resultados do estudo de caso realizado envolveu a simulação de cinco cenários de redes de referência, sinalizando que a identificação de pontos críticos em uma rede óptica a partir de uma perspectiva de risco permite que os gerentes definam pontos de redundância mais efetivos na rede, além de justificar a adoção de ações que possam mitigar riscos, contribuindo de forma mais efetiva para a melhoria do processo de gerenciamento de serviços.

Foi realizado um exercício de validade de aparência (RUNERSON e HOST, 2008) e os resultados indicaram que o modelo é útil, preferível, completo e efetivo. No entanto, a validação completa é uma atividade que requer muitos anos e várias repetições. Os resultados de validação indicaram que os gerentes preferiram o modelo proposto sobre o processo de identificação de redundância de pontos críticos que eles atualmente usam. Foram realizadas entrevistas com onze gerentes de TI e seis gerentes de rede de provedores de serviços, onde o modelo foi apresentado, bem como os resultados das simulações. As quatro hipóteses (utilidade, preferência, completude e efetividade) do modelo proposto foram validadas, com as hipóteses negativas refutadas em um exercício de validade de aparência (RUNERSON e HOST, 2009), conforme os resultados mostrados na Tabela 11. Foi utilizada inferência estatística para testar as hipóteses (BERGER e DELAMPADY, 1987; CASELLA e BERGER, 2002). Um teste

estatístico binomial Casella e Berger (2002) com significância de 5% foi utilizado para produzir os resultados apresentados na Tabela 11. Os resultados indicam que o modelo é útil e adequado para resolver o problema da identificação de pontos críticos em redes ópticas. Pode-se reivindicar a validade do modelo. Os resultados do estudo de caso foram promissores e contribuíram para a pesquisa de gerenciamento de serviços.

Tabela 11 - Hipóteses para teste da validade de aparência do modelo

Hipóteses	**% Respondentes que acreditam**	**Existe evidência estatística para refutar a hipótese negativa?**
Preferência: Os gestores preferem o modelo proposto em relação à forma atual de identificação de pontos de redundância em redes	94	Sim
Utilidade: Os gestores consideraram o modelo útil.	100	Sim
Completude: Os gestores consideraram o modelo completo em relação aos seus objetivos.	88	Sim
Efetividade: Os gestores consideraram o modelo efetivo para suporte ao gerenciamento de redes ópticas.	94	Sim

A contribuição desta pesquisa consiste no próprio modelo, que pode mitigar os riscos no gerenciamento da rede óptica, melhorar a qualidade dos processos de gerenciamento de serviços e facilitar os esforços dos gerentes em atividades de gerenciamento de riscos relacionados às falhas de elementos de redes ópticas.

Através da utilização do modelo *ASP* pelos gestores (*ferramenta de software ASP*) durante o estudo de caso realizado, foi possível identificar a partir dos resultados das entrevistas, que a compreensão da complexidade que envolve o alinhamento com o negócio e os riscos envolvidos no processo de gerenciamento de falhas em redes ópticas favorece o alcance dos objetivos estratégicos da empresa, permite que a empresa priorize a alta disponibilidade e qualidade de sua rede óptica, além de ajudar a organização na tomada de decisão sobre o quanto investir em pontos de redundância.

6.2 TRABALHOS FUTUROS

As contribuições geradas por esta pesquisa são de nível prático (desenho e implementação de um modelo quantitativo para suporte ao processo de identificação e priorização de pontos críticos) e empírico (validação do modelo). A contribuição prática dada por este trabalho para os estudos em *BDIM* foi explorar o potencial que a modelagem baseada em risco para o negócio apresenta para o gerenciamento de falhas em redes ópticas.

O processo de validação do modelo foi baseado na percepção de sua utilidade por gestores de TI e redes. Como primeira limitação à realização desta pesquisa, aponta-se para restrições do ponto de vista orçamentário, de logística e, principalmente, de acesso a organizações e pessoas dispostas a viabilizar um processo mais rigoroso de validação.

A metodologia aqui adotada para a modelagem é um processo bastante iterativo, que demanda tempo e dedicação de todos os envolvidos. O esforço de modelagem, verificação e validação também demandou o acesso a dados históricos sobre gerenciamento de falhas em redes ópticas. Este acesso foi bastante restrito. Apenas a organização pesquisada disponibilizou seus dados. A falta de alinhamento estratégico entre os objetivos do negócio, de TI e, consequentemente, do gerenciamento de falhas existente na organização pesquisada fez com que os benefícios explorados no modelo ficassem restritos aos cenários avaliados.

Por conta de limitações de tempo, escopo e financiamento, o estudo realizado nesta pesquisa teve seu foco limitado às tecnologias de redes ópticas tradicionais, existentes no mercado, não tendo se aprofundado em relação às novas propostas identificadas na literatura, como por exemplo as novas redes de transporte (OTN) e a proposta de redes elásticas. Por se tratar de uma abordagem híbrida, que envolve aspectos nas áreas de redes ópticas, gerenciamento de serviços e principalmente de negócio, o desenvolvimento do modelo *ASP*, apresentado nesta tese, demandou pesquisa em áreas de conhecimento interdisciplinares.

São feitas as seguintes sugestões para trabalhos futuros:

- Replicar este estudo em outros cenários rede e negócios e em diversas empresas, considerando topologias próprias e novas propostas para redes ópticas identificadas na literatura. Deve-se buscar o uso de valores financeiros na estimativa de impacto, além de um estudo comparativo com os resultados apresentados nesta pesquisa;

- Explorar o potencial de modelos de simulação para a formação de gestores no gerenciamento de falhas em redes ópticas;
- Proceder a inclusão de um subprocesso formal para a análise de riscos no processo proposto para o modelo *ASP*;
- Proceder uma formalização matemática do mapeamento de alarmes e seus impactos para o negócio e estudos de validação; e
- Avaliar e considerar na análise de riscos do modelo, a proposta de acrescentar a estimativa do grau de risco gerado pela ocorrência de duas falhas simultâneas de elementos da rede, cuja ideia foi apresentada durante a pesquisa e considerada útil pelos gestores.

Ainda como trabalho futuro, a funcionalidade da ferramenta *ASP* poderia ser aprimorada para incluir um método baseado em consenso para apoiar a tomada de decisões em grupo, como em um *Comitê Gestor*, especificamente na atividade de gerenciamento de falhas em redes ópticas, na visão de risco e perdas comerciais relacionadas.

REFERÊNCIAS

ABREU, F. de A.; FERNANDES, A. A.; **Implantando a Governança de TI: da estratég à gestão dos processos e serviços.** Rio de Janeiro: Brasport, 2006.

AGGELOU A. G. **Wireless Mesh Networking**. McGraw-Hill Professional, 2008.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002 –** Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação. Rio de Janeiro, ABNT, 2005.

BARLAS, Y. Multiple tests for validation of system dynamics type of simulation models. **European Journal of Operational Research**, v. 42, n. 1, p. 59-87, 1989.

BARTOLINE, C.; SAUVÉ, J. P. **Business driven it management.** businessdrivenitmanagemente.org, Disponível em :< http://www.businessdrivenitmanagement.org/ :1{8, 2008>. Acesso em 01 ago. 2008.

BARTOLINI, C. **Business-driven IT Management**. PhD thesis, Universitàdegli Studi di Ferrara, Italy, 2009.

BARTOLINI, C.; SALLÉ, M. **Business driven prioritization of service incidents.** L5th IFIP/IEEE International Workshop on Distributed Systems, 1:1-8, 2008.

BENHCINE, T.; HALIMA, E.; KARIM, I. **"Fast Reroute-based network resiliency experimental investigations."** Transparent Optical Networks (ICTON), 2013 15th International Conference on. IEEE, 2013.

BERGER, O.; DELAMPADY, M. **Testing precise Hypotheses**, Statistical Science 2, 1987.

BERRY, L. A conceptual model of service quality and its implications for future research. **Journal of Marketing**, v. 49, n. 4, p. 41-50, 1985.

BERRY, L. L.; PARASURAMAN, A. **Serviços de Marketing: competindo através da qualidade**. 3. ed., São Paulo: Maltese, 1991.

BEZERRA, R.; MOURA, A.; LIMA, A. S. **A system dynamics model to support strategic decision making on IT outsourcing:** A case study at a state revenue agency in Brazil. In: 2014 IEEE/IFIP Network Operations and Management Symposium, 2014.

BLOOMFIELD, E.;POPOV, P. ; SALAKO, K. ; STANKOVIC, V. ; WRIGHT, D. **Preliminary Interdependency Analysis:** An Approach to Support Critical Infrastructure Risk Assessment, Reliability Engineering and System Safety. 2017, doi: 10.1016/j.ress.2017.05.030.

BOULOUTAS, A.T. *et al*., Alarm correlation and fault identification in communication networks, **IEEE Trans. Commun**., v. 42, 1994.

CASELLA, G.; BERGER, R. L**. Statistical Inference,** 2 e., Duxbury Advanced Series, California, 2002.

FABRVENISTE, A. B.; HAAR, S.; JARDE, C.; AGHASARYAN, A. **Algorithms for Distributed Fault Management in Telecommunications Networks**, 11th International Conference on Telecommunicatons (ICT'2004), 2004.

FEN, Z.;YANQIN, Z.; LI, C. **Research on Metro Intelligent Optical Network Planning and Optimization**, 15th International Conference on Optical Communications and Networks (ICOCN), 2016.

FINN, S. G.; MERDARD, M.; BARRY, R. A. **A new algorithm for bi-directional link self-healing for arbitrary redundant networks**. Proceedings of Optical Fiber Communication Conference and Exhibit, Technical Digest, 1998, DOI: 10.1109/OFC.1998.657416.

GARDNER, R. D.; HARLE, D. A. **Network Fault Detection:** A Simplified Approach to Alarm Correlation, PS410, 1997. Disponível em http://citeseerx.ist.psu.edu/viewdoc/versions?doi=10.1.1.24.216. Acesso em: 22 out. 2007.

GOMES, T. *et al*., **Resilient routing in optical networks using SRLG-disjoint path pairs of min-sum cost,** Telecommun Syst ,V. 52, pp 737–749, 2013.

GÓMEZ, M.; MORA, M.; RAISINGHANI, M. S.; NEBEL, W.; O'CONNOR, R. V. **Engineering and Management of Data Centers: An IT Service Management Approach**, Springer, 2017.

Hicorp Comunicações Corporativas. **Gerência de Rede**. Junho, 2002.

HOMMA, Mitsunobu; SHINOMIYA, Norihiko. **"Finding Tie-sets with the Minimal Number of Total Elements for Effective Failure Recovery."**Proceedings of the 7th International Conference on Computing Communication and Networking Technologies. ACM, 2016.

HOUCKS, K.; CALO, S.; FINKEL, A. **Towards a practical alarm correlation system**. In IFIP/IEEE International Symposium on Integrated Network Management, IV (ISINM'95), pp. 226-237, 1995.

ISACA. COBIT 5 - **A Business Framework for the Governance and Management of Enterprise IT**. ISACA, Rolling Meadows-USA, 2015.

JAKOBSON, G; WEISSMAN, M. **Real-time telecommunication network management: extending event correlation with temporal constrainsts**. In IFIP/IEEE International Symposium on Integrated Network Management, IV (ISINM'95), páginas 290-301, 1995.

KAVIAN, Y. S.; RASHVAND, H. F.; LEESON, M. S; REN, W.; HINES, Evor L.; NADERI, M.. **Network Topology Effect on QoS Delivering in Survivable DWDM Optical Networks**, Journal of Telecommunications and Information Technology, v. 1, 2009.

KEHL, W.; HOPFMULLER, H. **Model-based reasoning for the management of telecommnunication networks.** In IEEE International Conference on Communications'93 (ICC 93), páginas 13-17, 1993.

KEUS, J. ; MARKUS, U. **Availability: Theory and Fundamentals for Practical Evaluation and Use**. 1063-9527/94, IEEE, 1994.

KLEINROCK, L. **Queuing Systems**, V. I: Theory. Wiley, New York, 1975.

LEE, K. ; CHO, E. **Characteristic for an Advanced Agent-Manager on the SDH Optical Network Management**, Network Operations and Management Symposium, NOMS 98, IEEE, pp. 354-363, 1998.

LEE, D.; LEE, L.; YOO, S.; RHEE, J. K. **Efficient Ethernet Ring Mesh Network Design**, Journal of Light Wave Technology, v. 29, n. 18, 2011.

LEHR, H. D.; ZEFFLER, P.; GLADISCH, A.; HANIK, N. **Management of All-Optical WDM Networks**, IEEE, pp. 870-879, 1998.

LI, C.; RAMASWAMI, R. **Automatic Fault Detection, Isolation, and Recovery in Transparent All-Optical Networks**, " IEEE Journal of Lightwave Technology, V. 15, n. 10, 1997.

LIA-XIA, L.; ZHANG, Y. **Design of a New EPON Connection Automatic Protection System**. P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2014 Ninth International Conference on. IEEE, 2014.

LIMA, A. S. **Modelo para Melhoria Contínua de Serviços de Tecnologia da Informação Sob o Ponto de Vista do Negócio.** Tese de Doutorado, Universidade Federal do Ceará, CE, 2011.

MACHUCA, C. M. **Fault localisation algorithms for optical networks**, Ph.D dissertation 2164, EPFL, 2000.

MACHUCA, C. M.; THIRAN, P. **A Review on Fault location Methods and their application to optical networks**. Optical network magazine, v. 2, pp. 73-87, 2001.

MACHUCA, C. M.; THIRAN, P; LEBOUDEC, J. **Fault location at the WDM Layer.** Photonic Network Comm, v. 1, n. 3, pp. 235-255, 1999.

MACHUCA, C. M; THIRAN, P. **An Efficient Algorithm for Locating Soft and Hard Failures in WDM Networks**, IEEE Journal on Selected Areas in Communications, v. 18, n. 10, 2000.

MALIK, A.; AZIZ, B.; ADDA, M.; KE, C. **Optimatisation Methods for Fast Restoration of Software-Defined Networks**, Access IEEE, v. 5, pp. 16111-16123, 2017, ISSN 2169-3536, 2017.

MALTZ, A; YUAN, L.; ZHANG, M; WU, X.; TURNER, D. J.; CHEN, C. **Automated datacenter network failure mitigation**, U.S. Patent US 9,025.434 B, issued May 5, 2015.

MAREK, W.G. **Power and beauty of interval methods. Domestic Conference on Evolutionary Algorithms and Global Optimization**, Poland, arXiv:pliysics/0302034v2:8pp, May 26-29, 2003.

MARQUES, F. T. **Projeto de Infra-estrutura de TI pela Perspectiva de Negócio**. Dissertação de Mestrado. Campina Grande, Universidade Federal de Campina Grande, 2006.

MARQUES, F. T; SAUVÉ, J.; MOURA, A. SLA design and service provisioning for outsourced services. **Journal of Network and Systems Management**, V. 17, Issue 1-2:73 - 90, 2009.

ḾEDARD, M. Redundant Trees for Preplanned Recovery in Arbitrary Vertex-Redundant or Edge-Redundant Graphs. **IEEE/ACM Transactions on Networking**, v. 7, n. 5, 1999.

MEIRA, D. **Um Modelo Para Correlação de Alarmes em Redes de Telecomunicações**. Phd Thesis, 621.39, Instituto de Ciências Exatas da UFMG, 1997.

MINES, J. A. **Overview of the Telecommunications Management Network**. In IEEE Global Telecommunication Conference (GLOBECOM 87), pag 1245-1248, 1987.

MOLLER, M; TRETTER, S.; FINK, B. **Intelligent filtering in network management systems**. In: Sethi A.S., Raynaud Y., Faure-Vincent F. (eds) Integrated Network Management IV. IFIP — The International Federation for Information Processing. Springer, Boston, MA, 1995.

MORECROFT, J. D. W. **Strategic modeling and business dynamics: a feedback system approach**, John Wley & Sons, 2007.

MOURA, A. B. **A possibility theoretic model for decision support in business-driven it service portfolio financial management under uncertainty**. In HP OVUA, Marrakech, Marrocos, 2008.

NÓBREGA, D.; FENNER, G.; LIMA, A. S. A Risk Management Methodology Proposal for Information Technology Projects **IEEE Latin America Transactions**, v. 12, n. 5, pp. 643-656, 2014.

O'CALLAGHAN, M. **Incident Management: Human factors and minimising mean time to restore service**, 2010. Disponivel em:

<http://dlibrary.acu.edu.au/digitaltheses/public/adt-acuvp272.01032011/index.html>. Acesso em: 12 de mai. 2011.

OFFICE OF GOVERNMENT COMMERCE. **ITIL v3 (Information Technology Infrastructure Library)/Service Operation, Service Strategy, Service Design, Service Transition, Continual Service Improvement**. London: TSO, 2007.

OLIVEIRA, A. **Um Modelo Formal para Avaliar o Valor de Negócio e sua Aplicação no Contexto de Gestão e Governança de TI**. PhD Thesis, Tese de Doutorado, Universidade Federal de Campina Grande, PB, 2010.

OLIVEIRA, W. de; BRITO, A. E. M.; BRASILEIRO, F. V. **Projeto e Implementação de um Serviço de Detecção de Falhas Perfeito**, XXI Simpósio Brasileiro de Redes de Computadores, 2003.

OP Services, **11 KPIs do ITIL para Gerenciamento de Disponibilidade**, disponível em https://www.opservices.com.br/kpis-itil-gerenciamento-de-disponibilidade/, 2017. Acesso em: 15 de jan. 2018.

PROJECT MANAGEMENT INSTITUTE. **Guia do Conjunto de Conhecimentos em Gerenciamento de Projetos - PMBOK**. Quarta edição, Four Campus Boulevard, Newtown Square, PA 19073-3299 EUA, 2008.

RAMASWAMI, R.; SIVARAJAN, K. N. **Optical Networks – A Practical Perspective**, 2 e., Academic Press, California, 2001.

READ, D. **Utility theory from jeremy bentham to daniel kalmeman**. London School of Economics and Political Science, 9:ISBN No: 07530 1689, 2004.

RUNERSON, M. H. **Guidelines for conducting and reporting case study research in software engineering**, Springer: Empiric Software Eng., v. 14, pp.31-164, DOI 10.1007, 2009.

SASTE, P.; MARTIS, J. **"Converged OAM."** Proceedings of the Second International Conference on Computer and Communication Technologies. Springer, New Delhi, 2016.

SAUVÉ, J. P.; MARQUES, F. ; MOURA, A. ; SAMPAIO, M. ; JORNADA, J.; RADZIUK, E. **An Introductory Overview and Survey of Business-Driven IT Management.** First IEEE/IFIP BDIM, pp. 1-10, 2006.

SAUVÉ, J. P.; MARQUES, F. ; MOURA, A. ; SAMPAIO, M. ; JORNADA, J.; RADZIUK, E. **Sla design from a business perspective.** In DSOM, 2005.

SERGIO, C.; SOUZA, J. A.; GONÇALVES, A. L. Idea Identification Model to Support Decision Making. **IEEE Latin America Transactions**, v. 15, n. 5, 2017.

SHEN, G.; GUO, H.; BOSE, S. K. "Survivable elastic optical networks: survey and perspective," **Photonic Network Communications**, v. 31, n. 1, pp. 71–87, 2016.

SILVA, A. C.; FAGOTTO, E. A. M. Diagnóstico e tratamento de incidentes na rede de computadores, **Anais...** da 11th International Conference on Information Systems and Technology Management – CONTECSI, 2014.

SMITH, P.; HUTCHISON, D.; STERBENZ, J. P.; SCHOLLER, M.; FESSI, A.; KARALIOPOULOS, M.; LAC, C.; PLATTNER, B. Network resilience: a systematic approach. **Communications Magazine,** IEEE, 49(7):88–97, 2011.

SOUSA, A. B.; DELFINO, C.; SOUZA, J. N.; BESSA, J. E. **An Algorithm for Fault Location in SDH/WDM Networks.**12th International Conference on Telecommunicatons (ICT'2005), 2005.

SOUSA, A. B. **Localização de Falhas em Redes de Comunicações Ópticas.** Dissertação de Mestrado, Universidade Federal do Ceará, CE, 2005.

SPECIALSKI, E. S. **Gerência de Redes de Computadores e de Telecomunicações,** white paper, Universidade de Santa Catarina, Florianópolis, 2018. Disponível em http://cassio.orgfree.com/disciplinas/gredes/ApostilaGerenciamento.pdf

STEIN, K. **"Redundancy-optimized communication network for the transmission of communication signals"** U.S. Patent US5946294 A, issued August 31, 1999.

STERBENZ, J. P.; HUTCHISON, D.; CETINKAYA, E. K.; JABBAR, A.; ROHRER, J. P.; SCHOLLER, M.; SMITH, P. Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. **Computer Networks**, 54(8):1245–1265, 2010.

Telecommunication Standardization Sector of the International Telecommunications Union. **Recommendation M.3000**: Overview of TMN recommendations, Outubro, 1994.

Telecommunication Standardization Sector of the International Telecommunications Union. **Recommendation M.3010.** Principles for a telecommications management network. ITU-T Recommendation, Fev 2000.

Telecommunication Standardization Sector of the International Telecommunications Union. **Recommendation** M3100. Generic Network Information Model, 1995.

Telecommunication Standardization Sector of the International Telecommunications Union. **Recommendation** X.720: Information technology – Open Systems Interconnection – structure of management information: Management information model, Janeiro 1992.

Telecommunication Standardization Sector of the International Telecommunications Union. **Recommendation** X710: Common Management Information Protocol specification for CITT applications, 1991.

THYAGATURU, A. S. Software defined optical networks (SDONs): A comprehensive survey. **IEEE Communications Surveys & Tutorials** v. 18, n. 4, pp. 2738-2786, 2016.

VASCONCELOS, M. F.; SALLES, R. M. Emprego de Resiliência na Gerência de Redes de Computadores, **Anais…** do XXX Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos, pp. 596-609, 2012.

WANG, Z.; ZHANG, M.; WANG, D.; SONG, C.; LIU, M.; LI, J. ; LOU, L.; LIU, Z. Failure prediction using machine learning and time series in optical network. **Optics Express**, v. 25, Issue 16, pp. 18553-18565 (2017) Disponível em: https://doi.org/10.1364/OE.25.018553. Acesso em: 30 de mar. 2018.

WEILL; J. W. Ross. **Governança de TI - Tecnologia da Informação**. Makron, 2006.

YEMINI, A.; KLIGER, S.; MOZES, E.; YEMINI, Y.; OHSIE, D. High Speed and Robust Event Correlation, **IEEE Communications Magazine**, 1996.

YIN, K. Case Sudy Research and Applications. **Design and Methods**, Sixth Edition, SAGE Publications, 2018.

ZADEH, L. **Rizzy sets as a basis for a theory of possibility**. Fuzzy Sets and Systems, 1:3-28, 1978.

ZEITHAML, V. A. **Delivering Quality Services: balancing customer perceptions and expectations**. New York: The Free Press, (1990).