PONTIFÍCIA UNIVERSIDADE CATÓLICA DE CAMPINAS

CENTRO DE CIÊNCIAS EXATAS, AMBIENTAIS E DE TECNOLOGIAS

MESTRADO PROFISSIONAL EM GESTÃO DE REDES DE TELECOMUNICAÇÕES

ALMIR CARLOS DA SILVA

MÉTODO PARA DIAGNÓSTICO E TRATAMENTO DE INCIDENTES EM SISTEMAS DE TELECOMUNICAÇÕES

PUC-CAMPINAS

2014

ALMIR CARLOS DA SILVA

MÉTODO PARA DIAGNÓSTICO E TRATAMENTO DE INCIDENTES EM SISTEMAS DE TELECOMUNICAÇÕES

Dissertação apresentada ao Curso de Mestrado Profissional em Gestão de Redes de Telecomunicações do Centro de Ciências Exatas, Ambientais e de Tecnologias da Pontifícia Universidade Católica de Campinas como requisito parcial para obtenção do título de Mestre em Gestão de Redes de Telecomunicações.

Área de concentração: Gestão de Redes e Serviços em Telecomunicações

Orientador: Prof. Dr. Eric Alberto de Mello Fagotto.

Dissertação defendida e aprovada em 30 de junho de 2014 pela Comissão Examinadora constituída dos seguintes professores:

_____

Prof. Dr. Eric Alberto de Mello Fagotto
Orientador da Dissertação e Presidente da Comissão Examinadora
Pontifícia Universidade Católica de Campinas

_____

Prof. Dr. David Bianchini
Pontifícia Universidade Católica de Campinas

_____

Prof. Dra. Marta Rettelbusch de Bastos

PUC-CAMPINAS

2014

Ficha Catalográfica

Elaborada pelo Sistema de Bibliotecas e

Informação – SBI – PUC-Campinas

T621.382 SILVA, ALMIR CARLOS DA.

S586M MÉTODO PARA DIAGNÓSTICO E TRATAMENTO DE INCIDENTES EM SISTEMAS DE TELECOMUNICAÇÕES / ALMIR CARLOS DA SILVA. - CAMPINAS: PUC-CAMPINAS, 2014.

77p.

Orientador: Eric Alberto de Mello Fagotto.

Dissertação (mestrado) - Pontifícia Universidade Católica de Campinas, Centro de Ciências Exatas, Ambientais e de Tecnologias, Pós-Graduação em Engenharia Elétrica.

Inclui bibliografia.

AGRADECIMENTOS

A Deus, autor e consumador de toda a vida, dono de toda a sabedoria e entendimento, e razão da minha existência, ao qual eu tenho por Senhor.

Ao Prof. Dr. Eric Alberto de Mello Fagotto, pelas inumeráveis lições de conhecimento transmitidas, e por me instruir na arte da ciência e pesquisa.

Aos Professores, Prof. Dr. Marcelo Abbade, Prof. Dr. Omar Branquinho, Prof. Dr. David Bianchini, Prof. Dr. Alexandre Mota e à Profa. Dra. Lia Mota pelas aulas ministradas e pelo conhecimento recebido.

À minha esposa Meire pela paciência, amor e companheirismo durante essa jornada, e às minhas filhas Letícia e Larissa pela inspiração que cada olhar e sorriso me proporcionam na caminhada.

À minha Mãe Telma Silva e ao meu Pai Janyr Silva, pelo exemplo que sempre foram para mim, e pelo apoio incondicional para formação do meu caráter e conhecimento, os quais me transformaram no que sou hoje.

À minha irmã, Me. Janize Maia e ao meu cunhado Me. Luiz Maia, por me incentivarem constantemente na busca do conhecimento, sendo para mim inspiração.

À minha tia, Dra. Stela Silva e ao meu tio Me. Gerson Silva pelo apoio, e pelo incentivo na obtenção desse título.

Aos colegas, Me. Marcelo Azevedo, em quem me inspiro na jornada do conhecimento, Tatiana Bernardes, que me apoiou na obtenção dos dados contidos no presente trabalho, bem como a todos os demais amigos que me apoiaram e incentivaram nessa caminhada, os quais se eu citasse cada nome, o espaço na presente dissertação não seria suficiente.

Ao meu diretor Daniel Galelli, pelo apoio e incentivo na conclusão desta etapa em minha vida.

À PUC Campinas pela concessão de bolsa de estudos para cursar o Mestrado.

"Bem-aventurado o homem que acha sabedoria, e o homem que adquire conhecimento."
Provérbios, 3:13

RESUMO

Em função da convergência de sistemas de voz, dados e serviços para uma mesma infraestrutura de telecomunicações, esta última se tornou essencial para os negócios e, portanto, qualquer indisponibilidade desta infraestrutura pode ocasionar sérios prejuízos e comprometer a imagem de uma companhia. Desta forma, na literatura recente, encontram-se relatadas estratégias voltadas à prevenção ou à minimização de falhas em sistemas de telecomunicações, em especial, naqueles que suportam missões críticas. Em vista de tal cenário, neste trabalho, apresenta-se um novo método para o diagnóstico e o tratamento de incidentes em sistemas de telecomunicações, baseado em uma sistemática que conjuga os modelos de eTOM e ITIL com quatro processos para: (i) o mapeamento de ambientes críticos, (ii) um procedimento de verificação de elementos de rede, o gerenciamento de incidentes, em tempo real, tanto (iii) em nível executivo como de (iv) suporte ao cliente.

Esta proposta foi implementada em clientes de uma provedora de serviços e sistemas de telecomunicações. Como resultado, verificou-se uma redução superior a 90% no número de incidentes abertos, em comparação com o período medido antes da implementação. Aplicando-se o método proposto aos demais clientes da empresa, foi possível solucionar mais de 50% dos incidentes. Tais resultados são apresentados e discutidos nesta dissertação, bem como as perspectivas de utilização futura da proposta.

ABSTRACT

The convergence of voice, data and services to the same telecommunications infrastructure systems, modified this last one to an essential element to the business and any unavailability in this infrastructure can cause serious business and financial issues and also damage the reputation of a company. Recent literatures reported strategies to prevent or minimize a failures impact in telecommunication systems particularly those that support critical missions. This paper presents a new method to the diagnosis and treat of incidents in telecommunication systems, based on a system that combine models of eTOM and ITIL with four processes to: (i) mapping critical environments, (ii) a procedure for verification of network elements, real-time incident management, in two perspectives: (iii) at the executive level (iv) and customer support.
This method was implemented in a customer of a telecommunications and systems services provider. The result was a greater than 90% reduction in the incident opened number compared to the measured period before implementation. Applying the method to other customers of the company the method was able to resolve over 50 % of incidents. These results are presented and discussed in this dissertation as well the next steps of the method development.

Sumário

ÍNDICE DE FIGURAS

ÍNDICE DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

AEIC = Acompanhamento Executivo de Incidentes Críticos

BPF = Business Process Framework

BSS = Business Support Systems

DC = Data Center

DV = Desktop Virtual

eTOM = Enhanced Telecom Operations Map

GB921V = Modelo do TMForum que Unifica o ITIL e o eTOM

ITIL = Information Technology Infrastructure Library

LVR = Lista de Verificação de Rede

MAC = Medium Access Control

MACN = Mapeamento de Ambiente Críticos ao Negócio

MALF = Sigla de MACN, AEIC, LVR e Fluxo

Modelo Z = Nome definido neste trabalho para o modelo concebido por Zhuang [1]

NGOSS = New Generation of Operations Systems and Software

OSS = Operations Suport Systems

RCA = Root Cause Analisys

TI = Tecnologia da Informação

TMF = Telecommunications Management Forum

TMN = Telecommunications Management Network

TOM = Telecomunications Operations Map

1. Introdução

Atualmente, os sistemas de telecomunicações sofreram transformações, tornando-se muito importantes e com grande relevância para os negócios de uma empresa [2]. Em tais empresas, a dependência destes sistemas para troca de informações e serviços, bem como o desenvolvimento de negócios que utilizam sua infraestrutura cresce a cada dia [3]. No entanto, poucas empresas aplicam algum método para estruturação de seus sistemas e mantém um controle do que é transmitido por eles pelos sistemas de telecomunicações [4]. Adicionalmente, não há um planejamento prévio para dimensionar o volume das aplicações que são transmitidas utilizando-se destes sistemas, bem como previsão de crescimento do número de usuários, janelas pré-estabelecidas de manutenção, monitoramento do tráfego para uma projeção estatística de crescimento e consequente planejamento de capacidade do ambiente das redes de telecomunicações [5]. Associada a esta realidade, está a migração das funcionalidades de serviços para a rede de telecomunicações como voz sobre IP, videoconferência e telepresença, monitoramento por câmeras de segurança e outros tipos de serviços para a rede e sistemas de comunicação [6]. Por outro lado, há uma tendência de cada vez mais, o negócio de uma empresa estar associado ao uso da infraestrutura de Tecnologia da Informação (TI) para seu funcionamento [7][8]. A utilização de equipamentos informatizados, tais como tornos, envasadeiras, centrífugas, de dispositivos móveis, conectados a sistemas de telecomunicações para prover interatividade e acesso a diversos conteúdos de informação, precisa e atualizada, para os negócios já é uma realidade em muitos cenários de empresas de todos os gêneros [9][10][11][12].

Como consequência deste cenário, verifica-se que qualquer falha ocasionada pelos sistemas de comunicação causa grandes problemas para os negócios da empresa [13]. Esforços apresentados na literatura concentram-se em aumentar a disponibilidade dos sistemas de telecomunicações e dos serviços nela contidos, bem como prover um rápido restabelecimento destes em caso de falhas [14][15][16][17]. Com o crescimento acelerado da concorrência entre empresas e negócios, garantir a disponibilidade de um serviço ou sistema pode representar vantagem competitiva [18]. Todavia, a indisponibilidade de tais serviços pode impactar diretamente na imagem da companhia e na forma como a sociedade vê e classifica essa empresa, além dos prejuízos financeiros que uma indisponibilidade da rede pode ocasionar [19]. De acordo com [20] a falha ou

indisponibilidade de um equipamento ou serviço é o estado ou o modo no qual o sistema não pode cumprir sua missão designada de forma satisfatória. Devido à importância que o ambiente de TI vem desenvolvendo, cada vez mais as empresas e o mercado em geral têm procurado utilizar modelos de melhores práticas para o ambiente de TI, com o objetivo de controlar a infraestrutura, assim como desenvolver mecanismos para prevenir, ou minimizar qualquer parada não planejada neste ambiente [21][22]. Efetuar o rápido reestabelecimento de um serviço nos dias de hoje é um desafio, e cada vez mais métodos que auxiliem neste processo, visando a diminuição de tempo no atendimento são escassos.

Neste trabalho é apresentada uma proposta de um método para diagnóstico e tratamento de incidentes baseado em dois dos métodos mais utilizados para a governança de TI. O primeiro é a Biblioteca de Infraestrutura da Tecnologia da Informação, conhecido pelo nome em inglês *Information Technology Infrastructure Library* (ITIL) e o *Mapa Avançado de Operações de Telecomunicações, também comumente conhecido por seu nome em inglês Enhanced Telecom Operations Map* (eTOM), os quais são apresentados e discutidos no capítulo 2. Apresenta-se a utilização do modelo GB921V [23], que aborda a convergência de ambos os modelos, e discutem-se os benefícios desta unificação de modelos. Neste trabalho foi utilizada a versão inicial do GB921V, por oferecer uma completa abordagem do modelo, bem como o detalhamento das diferenças entre ITIL e eTOM. Ainda no capítulo 2, é apresentado um modelo para o tratamento de incidentes, seu fluxo e funcionamento, e são realizadas considerações sobre o modelo. Nos capítulos 3 e 4*,* é apresentado um método para o diagnóstico e tratamento de incidentes em sistemas de telecomunicações, os processos que compõem a proposta, e o novo fluxo proposto para o gerenciamento de incidentes na operação de uma provedora de serviços de gerenciamento de rede e telecomunicações. A aplicação e validação do método proposto, com o detalhamento cada etapa do processo, está descrita no capítulo 5.

2. Gerenciamento de Processos para Serviços Convergentes baseados em ETOM e ITIL

Neste capítulo, discutem-se os modelos ITIL e o eTOM, o histórico e a motivação para a criação dos mesmos, bem como suas estruturas e componentes. Tais métodos monstraram-se eficientes se aplicados à oferta de serviços em sistemas de telecomunicações [24][25]. Seus modelos permitem a utilização de processos para a criação, manutenção e encerramento do ciclo de vida de um produto ou serviço. Adicionalmente, são compostos de processos para solucionar de maneira estruturada, problemas originados da migração de sistemas e serviços essenciais para as empresas na perspectiva de negócio, para sistemas de telecomunicações com uma infraestrutura única e abrangente. As estruturas do ITIL e do eTOM, atuando conjuntamente, permitem um gerenciamento completo da infraestrutura. Tal estruturação se mostra totalmente integrada ao modelo de serviços fornecidos em rede e sistemas de comunicação. O modelo GB921V [23] exibe a convergência dos métodos ITIL e eTOM, utilizando-se da estrutura em camadas e orientação a processos do eTOM juntamente com as melhores práticas abordadas pelo ITIL, provendo um novo modelo estruturado para o suporte de serviço e o suporte de entrega (*service support* e *service delivery*). No final do presente capítulo, discute-se um método concebido a partir da convergência dos métodos apresentados, a motivação para sua concepção, os fluxos propostos pelo modelo para o gerenciamento de incidentes, e considerações sobre o modelo.

2.1. Biblioteca de infraestrutura da tecnologia da informação

Atualmente, os serviços de TI tornaram-se parte do negócio das empresas e, como conseqüência, ganharam importância para tais negócios [18]. Mediante este cenário, verificou-se a necessidade do estabelecimento de modelos de administração da infraestrutura de TI, denominados de governança de TI, devido à criticidade que tal ambiente adquiriu para o negócio das empresas [26]. O uso destes modelos de

governança tem por objetivo administrar a infraestrutura, de maneira a potencializar a disponibilidade das mesmas, e um rápido restabelecimento em caso de falhas [27][28]. Desenvolveram-se métodos compostos com as melhores práticas utilizadas por diversas empresas para o ambiente de TI. Neste capítulo, discute-se a Biblioteca de Infraestrutura da Tecnologia da Informação, comumente conhecida como ITIL. Esta biblioteca foi criada pelo governo britânico em 1980, em uma pesquisa realizada com o objetivo de reunir as melhores práticas exercidas pelas maiores empresas da área de TI. Tornou-se um padrão em1990. Atualmente, este modelo é organizado e regulado pelo *IT Service Management Forum* (ITSMF)[29] e se tornou um padrão seguido por diversas empresas em âmbito mundial [30]. O objetivo do ITIL é ser um modelo que indica o que deve ser realizado na perspectiva das melhores práticas a serem utilizadas na gerência e gestão do ambiente de TI, no entanto sem especificar como tais ações devem ser implementadas [4]. O foco principal do ITIL é a operação e gestão da infraestrutura de tecnologia em uma empresa e se utiliza de diversos processos para tal, com finalidade de garantir que os serviços da tecnologia da informação estejam em acordo com as necessidades de negócio das empresas [31]. Importante ressaltar que o ITIL apresenta uma perspectiva de como os processos devem ser tratados dentro do universo de TI, sendo este é um dos grandes diferenciais, e a razão do sucesso do modelo. Devido a esta característica, o modelo se aplica a qualquer empresa seja ela pública ou privada, pequena ou grande, pois os processos propostos pelo modelo são genéricos e precisam ser adaptados ao perfil da empresa. Também não há dependência do parque tecnológico existente para que o modelo ITIL possa ser utilizado.

Segundo o fórum que desenvolve e mantém o ITIL [32], este modelo oferece um *framework* comum para as diversas atividades do ambiente de TI. Tais atividades são comumente divididas em processos que possibilitam um fluxo mais eficiente ao gerenciamento de TI. Cada processo engloba uma ou mais tarefas do ambiente de TI aplicado ao âmbito corporativo. Estes processos permitem utilizar as boas práticas adotadas e inseridas no modelo para adaptação ao ambiente de TI das diversas empresas, em seus mais diferentes ramos e campos de atuação. O modelo proposto pelo ITIL concentra-se em dois domínios basicamente. Tais domínios são apresentados na próxima seção.

2.1.1. Gerenciamento de Serviços– *Suporte*

Este domínio contempla atividades que são utilizadas no dia a dia para administração e mantenimento da infraestrutura de TI. Concentra-se em áreas que abordam as atividades comuns em uma estrutura de TI. São elas:

- ***Service Desk*** - Área de interação com o cliente, abertura de incidentes e requisições. Pode agregar outras funcionalidades como solicitação de mudanças, licenças de software, manutenções, dentre outras.
- **Gerenciamento de Incidentes –** Responsável por acompanhar e restaurar a operação normal de um serviço, garantindo sua disponibilidade e qualidade.
- **Gerenciamento de Problemas** - Responsável por identificar, e corrigir os erros no ambiente de TI, e também garantir que a solução de correção de um problema não torne a ocorrer.
- **Gerenciamento de Configuração** - Responsável por apoiar o gerenciamento do ambiente de TI, controlando componentes e alterações em tal ambiente.
- **Gerenciamento de Mudanças** - Responsável por controlar todas as janelas de manutenção ou mudanças que sejam realizadas no ambiente de TI garantindo que as mesmas ocorram de maneira segura e estruturada.
- **Gerenciamento de Versões** - Responsável por assegurar que apenas versões testadas e homologadas de software autorizado sejam disponibilizadas para a operação.

2.1.2. Gerenciamento de Serviços – Entrega *(Service Delivery)*

Este domínio concentra-se no planejamento e na melhoria dos serviços ofertados pela estrutura de TI. O modelo contempla o gerenciamento de processos que tem por objetivo avaliar e propor transformações nos mesmos para melhoria do modelo. São eles:

- **Gerenciamento do Nível de Serviço** - Responsável por medir se o nível de serviço acordado para um determinado serviço oferecido está sendo

cumprido, e caso não esteja, o que precisa ser alterado para que o objetivo se cumpra.

- **Gerenciamento de Capacidade** - Responsável por acompanhar a utilização de recursos a fim de planejar novas aquisições, bem como evitar problemas em decorrência de gargalos.
- **Gerenciamento Financeiro** - Responsável por controlar toda a questão de custos da infraestrutura de maneira que estes estejam alinhados ao negócio da companhia, bem como que os mesmos não venham a ultrapassar os valores planejados.
- **Gerenciamento de Disponibilidade** - Responsável por medir e garantir que a disponibilidade de recursos e serviços esteja em acordo com o que foi oferecido ao usuário, seja este um cliente, um departamento ou ainda um sistema.
- **Gerenciamento de Continuidade** - Responsável por identificar as ações que devem ser realizadas para o ciclo de vida de um serviço oferecido, seja este de oferecimento de um serviço, ou ainda a retirada do mesmo da operação.

Com a evolução do ITIL, no entanto, alguns aspectos foram transformados. Em sua terceira versão [32], o ITIL aborda novos ambientes em uma estruturação diferente da apresentada na seção 2.1.1 e 2.1.2. Estas estão divididas em:

- Estratégia de Serviços
- *Design* de Serviços
- Transição de Serviços
- Operações de Serviços
- Melhorias Contínuas de Serviços

Os domínios apresentados na versão 2.0 foram incorporados e distribuídos dentro da estrutura apresentada na versão 3.0, a qual ampliou a abrangência da área de TI no universo empresarial, estendendo o enfoque do ITIL frente aos demais departamentos de uma empresa, pois possui um alinhamento associado ao negócio oferecido pelas empresas, e interagindo com este, assim como entre os demais departamentos.

2.2. Mapa Avançado de Operações de Telecomunicações

Ainda na perspectiva da governança de TI, outro método que se destacou dentre os modelos existentes (*frameworks*) para a gerência de TI é o mapa avançado de operações de telecomunicações, comumente conhecido por eTOM [33]. Este teve sua criação como derivação de um modelo chamado *Telecommunications Management Network* (TMN), criado pela União Internacional de Telecomunicações (UIT) em 1988, como uma proposta de estabelecimento de padrões para a automação de processos operacionais em uma provedora de serviços telecomunicações [34]. O modelo proposto pelo TMN permitiu introduzir padrões para recursos utilizados nas funções ou processos de cada camada existente no modelo, estabelecendo padrões de interfaces e a interoperabilidade de equipamentos e sistemas. A Figura 1 mostra o modelo TMN relativo à Gerência Integrada de Redes e Serviços.

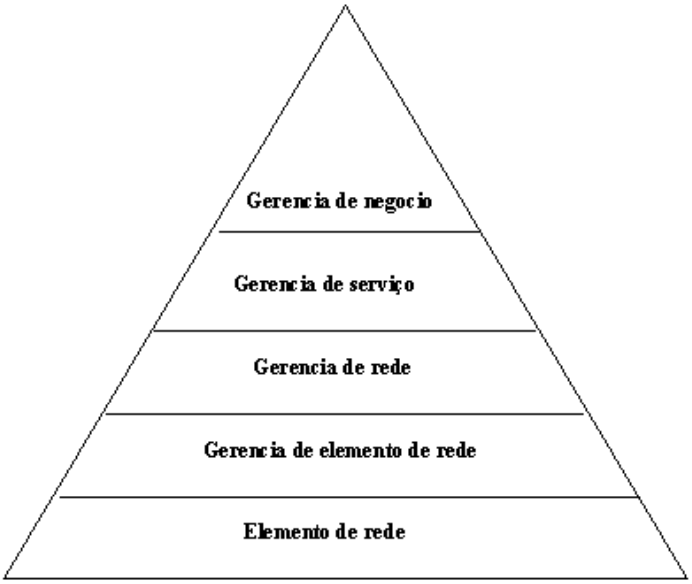

Figura 1 – Modelo TMN – Gerência Integrada de Redes e Serviços – Fonte: Teleco (www.teleco.com.br)

Na Figura 1 é apresentada a pirâmide de gerência de rede, que tem como base o elemento de rede, que somado aos demais equipamentos da rede e dos sistemas de telecomunicações representam a infraestrutura. Imediatamente acima, está a gerência do elemento de rede. Esta tem por missão efetuar todo o controle dos equipamentos e sistemas existentes. Imediatamente acima deste nível, está a gerência da rede. Possui uma visão sistêmica da infraestrutura e dos serviços fornecidos por ela. Neste nível há também a gestão, ou seja, ocorrem as tomadas de decisão sobre a utilização, alteração ou atenção com investimentos que necessitam ser feitos nos sistemas de

telecomunicações. No topo da pirâmide está a gerência de negócio. Esta é a razão da existência dos níveis inferiores. Neste nível está localizada a necessidade de negócio, e é mediante tal necessidade que a infraestrutura é dimensionada e preparada, para então ofertar os serviços que irão atender os clientes.

Criaram-se dois grupos de sistemas para suportar os processos operacionais de uma provedora de serviços de Telecomunicações:

- ***Business Support Systems*** (BSS) – Trata-se do sistema de suporte ao negócio, envolvendo Billing e CRM.
- ***Operations Support Systems*** (OSS) – Trata-se do sistema de suporte à operação, que envolve todos os sistemas que são utilizados para suportar a operação da rede.

Atualmente o modelo é estabelecido e mantido pelo Telecommunications Management Network (TMF), e o modelo atualmente em uso é o Mapa de Processos de Negócio, comumente conhecido por seu nome em inglês, Business Process Framework (BPF)[35], criado em 2012. Segundo o TMF, o BPF é um catálogo hierárquico dos principais processos de negócios necessários para gerir uma empresa focada no serviço. Em nível conceitual, o quadro tem três grandes áreas de processos, refletindo maiores focos dentro de empresas típicas:

- Estratégia, Infraestrutura e Produto
- Operações
- Gestão Empresarial

O BPF é denominado o coração do modelo que recebe o nome de Frameworx, um completo guia para permitir o sucesso da transformação de negócios. Segundo o TMFORUM o modelo é a única forma padronizada dentro da indústria de telecomunicações para capturar processos de negócio. Alguns dos objetivos do modelo são:

- Criar uma linguagem comum para uso em departamentos, sistemas, parceiros externos e fornecedores, reduzindo custos e riscos de implementação do sistema, integração e aquisição;
- Adotar um esquema de estrutura, terminologia e classificação padrão para processos de negócios para simplificar as operações internas e maximizar as oportunidades de parceria dentro e entre as indústrias;

- Aplicar o desenvolvimento de processos de negócios disciplinada e consistente em toda a empresa, permitindo a reutilização inter-organizacional;
- Entender, projetar, desenvolver e gerenciar aplicações em termos de requisitos de processos de negócios para que os aplicativos irão melhor atender as necessidades do negócio;
- Criar fluxos de processos consistentes e de alta qualidade, eliminando falhas e duplicações;
- Identificar oportunidades de custos e melhoria de desempenho, através da reutilização de processos e sistemas existentes;

O BPF possui sete grupos de processos verticais nas áreas de Estratégia, Infraestrutura e Produtos, e Operações. Esses grupos verticais de processos têm como foco atividades em sua totalidade. Cada grupo possui processos envolvendo clientes, suportando serviços, recursos e provedores/parceiros. Tais grupos verticais podem ser idealizados como um ciclo de vida quando visualizados da esquerda para direita na Figura 2. O presente trabalho concentra-se na camada denominada Gerenciamento de Serviços e operações (*Service Management & Operations*), no processo vertical responsável pelo Suporte da Operação e a disponibilidade da mesma. Esta camada é responsável por todos os processos que objetivam a disponibilidade dos serviços para o usuário, englobando os processos de gerenciamento de incidentes e requisições de serviço. Todos estes pontos estão inseridos na área de Operações apresentada na Figura 2.

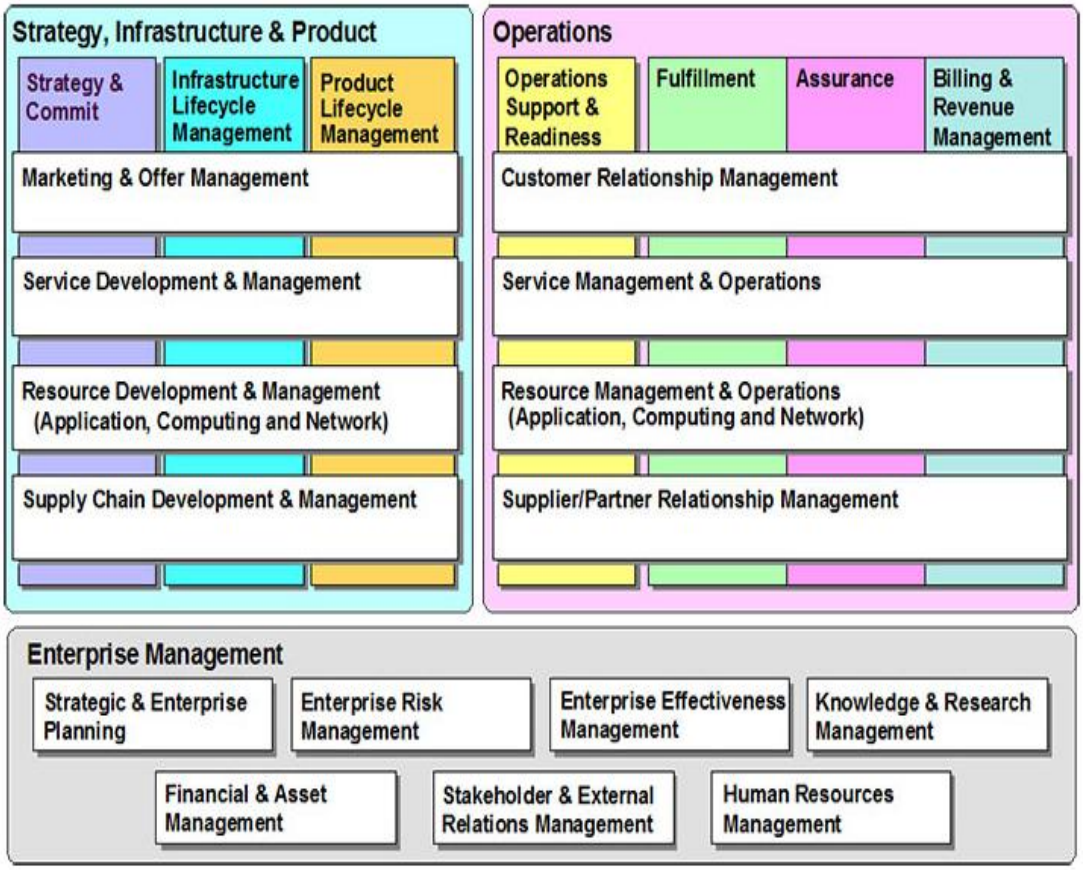

Figura 2–Mapa de processos de negócio proposto pelo BPF. Fonte: TMForum (http://www.tmforum.org)

Há ainda outro grupo como base do modelo, que é o grupo de Gerenciamento Empresarial. Nele estão contidos diversos processos relativos à gestão, como Planejamento Empresarial e Estratégico, Gerenciamento de Risco Empresarial, Gerenciamento de Efetividade Empresarial, Gerenciamento de Pesquisa e Conhecimento, Gerenciamento de Ativos e Finanças, Gerenciamento de Relações Externas e Investidores e Gerenciamento de Recursos Humanos. Todos estes itens apresentados na Figura 2 não são processos da infraestrutura de serviços ou de TI, mas esta é influenciada ou diretamente afetada pelas decisões efetuadas nesse grupo.

A utilização do *framework* proposto pelo BPF permite que cada camada seja amadurecida e evolua de maneira independente do processo como um todo. Novas propostas e agregações ao modelo podem ser realizadas somente na etapa na qual o processo está definido, sem que seja necessária uma readaptação de todo o *framework*. Esta é uma das razões pelas quais o setor e as empresas adotaram o uso do modelo para suas operações. Atualmente, outros tipos de empresas e provedores de serviços adotaram o BPF como referência para o amadurecimento de processos e refinamento de

serviços oferecidos [36]. Atualmente o TMF possui mais de 700 membros em mais de 75 países mediante a convergência das indústrias de Telecomunicações, cabeamento, mídias e Internet.

2.3. Convergência entre eTOM e ITIL – GB921V

Para entender a relação entre eTOM e ITIL é preciso entender os diferentes termos utilizados em cada modelo. Em muitos casos existem termos com o mesmo nome, no entanto com diferentes significados. Um exemplo de tal diferença está no significado de “problema”. Para o ITIL, “problema” significa uma falha que necessita de investigação, mediante processos os quais possuem um fluxo para a identificação da causa raiz e sua conseqüente solução, bem como medidas para que o problema não volte a acontecer. Na visão do eTOM, um “problema” está relacionado à identificação de uma falha em algum elemento do *framework* [23].

A seguir são mostradas algumas diferenças de abordagem entre os modelos.

- eTOM
  - Contexto de negócio totalmente moldado para Provedores de Telecomunicações
  - Padronização internacional baseada no ITU
  - Constituído da seção de visão de negócio da NGOSS, uma iniciativa da TMF em soluções OSS / BSS
  - Linguagem comum para processos de negócio
  - Uma hierarquia para definições de processo
  - Um repositório de elementos de processo com vários níveis de detalhes que podem ser combinados e aplicados em situações especificas
  - Provê exemplos de fluxos de processos
  - Diagramas de fluxo são utilizados no eTOM para demonstrar processos fim-a-fim
  - Conteúdo técnico maduro, com uma ênfase aumentada em referências para aplicação e uso

- ITIL
  - Incluído em vários padrões nacionais e é parte da ISO
  - Um abrangente e consistente conjunto de boas práticas

- Um conjunto de métodos para entrega otimizada e controlada de serviços
- Linguagem comum. Ex: Incidente é utilizado em qualquer evento que cause a interrupção ou redução de um serviço
- Objetivo de fornecer alta qualidade de serviços com um foco particular em relacionamento com o cliente
- É construído em acordos, onde a organização de TI pode atuar se estiver em comum acordo com o cliente
- O processo de entrega de serviço e parcialmente preocupado com a criação de acordos e monitora os prazos estabelecidos para esses acordos. No nível operacional, o processo de suporte dos serviços precisa ser visualizado como entrega de serviço, assim como previsto nos acordos.
- Apresentações de fluxo são utilizadas no ITIL
- Inclusão dos ciclos de retorno da qualidade para melhoria contínua
- Suporte e direcionamento da qualidade repetidamente

Mediante as diferenças entre eTOM e ITIL, questionou-se sobre o porquê convergir os modelos. É reconhecido que empresas que se utilizam da abordagem adotada pelo modelo estão preparadas para as mudanças de circunstâncias e os respectivos benefícios de negócio. Da mesma forma, empresas expostas a ambos os modelos precisam possuir conhecimento para integrar estas abordagens. A combinação dos modelos pode possibilitar uma entrega melhorada de valor de negócio.

Em 2005 o TMFORUM publicou o modelo GB921V, que efetua a convergência das melhores práticas contidas no ITIL com a estruturação em camadas do eTOM. O objetivo foi proporcionar uma visão de negócio da abordagem convergente dos modelos, oferecendo um apoio mútuo dos métodos para o melhor aproveitamento dos processos para o negócio das empresas.

2.4. Um modelo de gerenciamento para serviços convergentes

Com o objetivo de minimizar o tempo de indisponibilidade da operação dos sistemas de telecomunicações, bem como de prevenir falhas, [1] desenvolveram um modelo baseado no GB921V para o gerenciamento de processos para serviços convergentes. Este método será tratado neste trabalho como modelo Z, para uma clara diferenciação dos modelos apresentados.

O modelo Z propõe um método otimizado para processos de gestão e serviços convergentes em sistemas de telecomunicações. O objetivo da elaboração deste método segundo o autor foi atender aos requerimentos de gerenciamento que surgem com a migração de serviços de diferentes características para o mesmo meio de comunicação, requerendo um gerenciamento abrangente, além de soluções para as expectativas de uma integração completa na nova infraestrutura. Tal método foi constituído para atender os requerimentos de serviços convergentes, destacando-se:

- Unificação dos termos, pois há uma diferenciação nos termos relacionados para serviço, erro, mudança e configuração entre eTOM e ITIL.
- Elemento do processo. Como no eTOM, o método se molda a um elemento do processo, atendendo o processo fim a fim como na perspectiva de serviço completo (*full-service perspective*)
- Estrutura em camadas: A estruturação em camadas representa a elaboração das características empresariais, e o ITIL não possui tal estruturação, nativa do eTOM. Cada camada pode ser interpretada como um único meio de negócio no âmbito corporativo. As camadas interagem entre si e há uma perspectiva de futuro que a evolução das camadas venha a incrementar a eficiência do processo de gerenciamento.

De acordo com o autor, a principal idéia da convergência está na formação de um modelo de processo estabelecido a partir da necessidade de negócio dos provedores de serviço, e utilizá-los para conceber uma série de fluxos processuais compatíveis com o modelo do eTOM. O ITIL por sua vez irá observar as necessidades práticas, e organizá-las em um modelo que possa abranger as áreas de entrega de serviços de TI, e o apoio de tais serviços. As boas práticas do ITIL são então utilizadas para possibilitar que os fluxos do eTOM estejam alinhados com tais requerimentos. O resultado é um modelo criado com base no cenário de serviços convergentes e é apresentada a seguir:

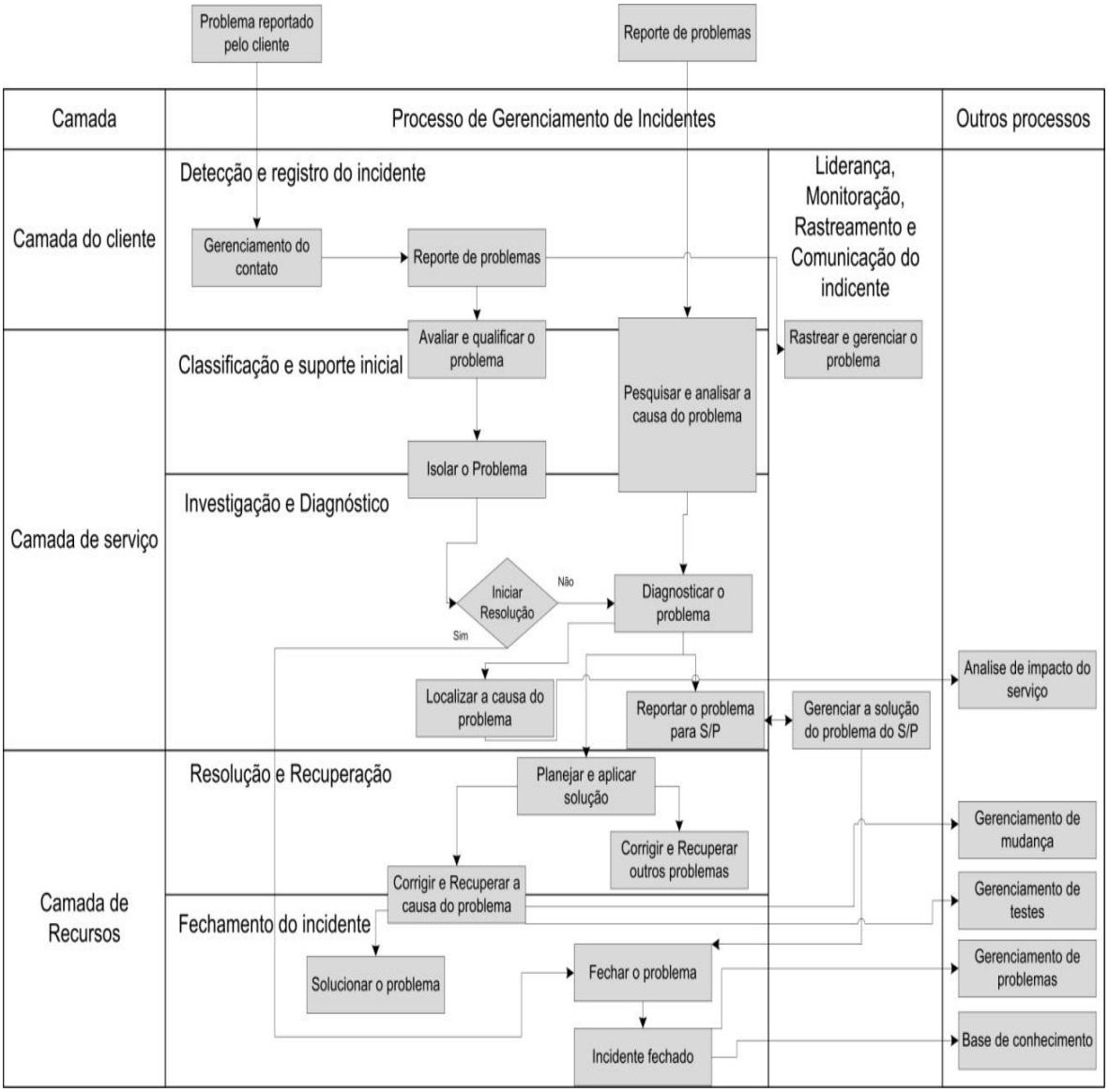

Figura 3 – Diagrama de blocos apresentando o fluxo proposto por [1] para tratamento de incidentes.

A Figura 3 exibe um diagrama de blocos que demonstra o fluxo para o gerenciamento de incidentes proposto pelo modelo Z, o qual se utiliza da estrutura em camadas, pois proporciona uma redução da complexidade comumente observada nos métodos de gerenciamento de rede corporativos [37]. É composto de três camadas, que possuem elementos que constituem o processo de gerenciamento de incidentes. Tais camadas são explicadas na sequência.

- **Camada do cliente** - Composta por uma etapa de detecção e registro de incidentes, que basicamente faz o gerenciamento do contato com cliente e o reporte do problema, e o direciona para qualificação.
- **Camada de Serviço** - A camada de serviço é composta por duas etapas: uma etapa de classificação e suporte inicial, onde é realizada a qualificação do problema reportado pelo cliente e então se inicia a segunda etapa, que é a Investigação e Diagnóstico, onde é realizado o diagnóstico e localização do problema. Estando o mesmo relacionado com algum provedor de serviço, o reporte para o mesmo também é realizado nessa etapa.
- **Camada de Recursos** - A camada de recursos é constituída por duas etapas: A primeira de resolução e recuperação, na qual ocorre o planejamento e a aplicação da correção ou solução do problema, e a etapa de fechamento do incidente, na qual devem ser documentadas as ações para correção do problema, e o fechamento do incidente.

As etapas descritas nas camadas apresentadas fazem parte de um processo para gerenciamento de incidentes, o qual possui, adicionalmente, uma etapa denominada Liderança, Monitoração, Rastreamento e Comunicação do Incidente, que está inserida no fluxo e em paralelo a todas as camadas apresentadas. Esta etapa sugere ao modelo Z, uma proposta de *cross-layer,* que são violações ao modelo tradicional da estruturação em camadas. Mediante essa abordagem, uma camada não precisa obrigatoriamente se comunicar com outra através da camada subseqüente, propondo uma nova forma de comunicação [38]. A Figura 3 propõe a interação da etapa de Liderança, Monitoração, Rastreamento e Comunicação do Incidente com todas as demais camadas apresentadas na tabela 3 em diversas situações, pois se entende que o gerenciamento do problema, bem como o rastreamento do mesmo pode ocorrer em quaisquer das etapas e camadas descritas no modelo Z. Nesta etapa também está proposta a interação junto ao provedor de serviços, caso a solução do problema esteja relacionada com algum serviço fornecido por uma empresa terceira. Há outra etapa semelhante à anterior, com a mesma abordagem de *cross-layer*, na qual estão inseridos alguns fluxos previstos no ITIL, como análise de impacto do serviço, gerenciamento de mudanças, gerenciamento de testes, gerenciamento de problemas e por fim a etapa de documentação do incidente em uma base de conhecimento, para consulta futura. A estrutura de camadas utilizada no modelo Z obedece a mesma organização em camadas prevista no modelo do eTOM para gerenciamento de serviços, além das implementações do fluxo e das melhores práticas

previstas no ITIL para gerenciamento de incidentes, otimizando desta forma, segundo [1], o diagnóstico e o tratamento do problema. Tal otimização apresentada se dá mediante a definição de uma análise de requisitos do processo de gerenciamento de incidentes previsto no ITIL. Como resultado constituiu um fluxo de procedimentos que trabalham em uma abordagem de cima para baixo, além de delimitar o terceiro elemento do processo de estrutura do eTOM, complementando e atualizando os elementos do processo de acordo com os requerimentos atuais.

2.5. Considerações sobre o modelo Z

Após uma análise realizada no modelo apresentado, observaram-se algumas considerações no fluxo proposto. Tais considerações são classificadas a seguir:

- **Rastreamento do problema** – Identificou-se na camada do cliente a abertura de um registro relatando um problema. Existe no diagrama de blocos apresentado no modelo de [1] um processo vertical nominado de Investigação Liderança, Monitoração, Rastreamento e Comunicação do Incidente. Neste processo, conforme a sequência do fluxo proposto no modelo Z, é realizado o rastreamento e gerenciamento do problema, identificado na Figura 4 pelo número 1. Verificou-se neste processo uma falta de sequência no fluxo proposto quanto ao rastreamento do problema, pois não são apresentadas na sequência do fluxo, continuidade na identificação e solução do problema, bem como não foi possível verificar a etapa de documentação e encerramento do incidente como término do processo.
- **Interação com o cliente** – Notou-se que a etapa de rastreamento e gerenciamento do problema não prevê uma interação com o cliente para administração de uma crise ocasionada por um incidente relacionado ao negócio do mesmo.

Tal ponto demonstrou-se relevante se observado que o método é baseado na convergência entre o ITIL e o eTOM, e ambos têm como foco principal o cliente, como já observado na descrição dos modelos apresentada no capítulo 2. Identificou-se claramente a utilização das estruturas do ITIL e do eTOM na construção do modelo Z, no entanto não é possível perceber uma implementação completa dos processos descritos na estrutura de ambos nos fluxos apresentados no diagrama de blocos proposto pelo

modelo Z, e conseqüentemente os benefícios que tais ações proporcionam para o gerenciamento de incidentes.

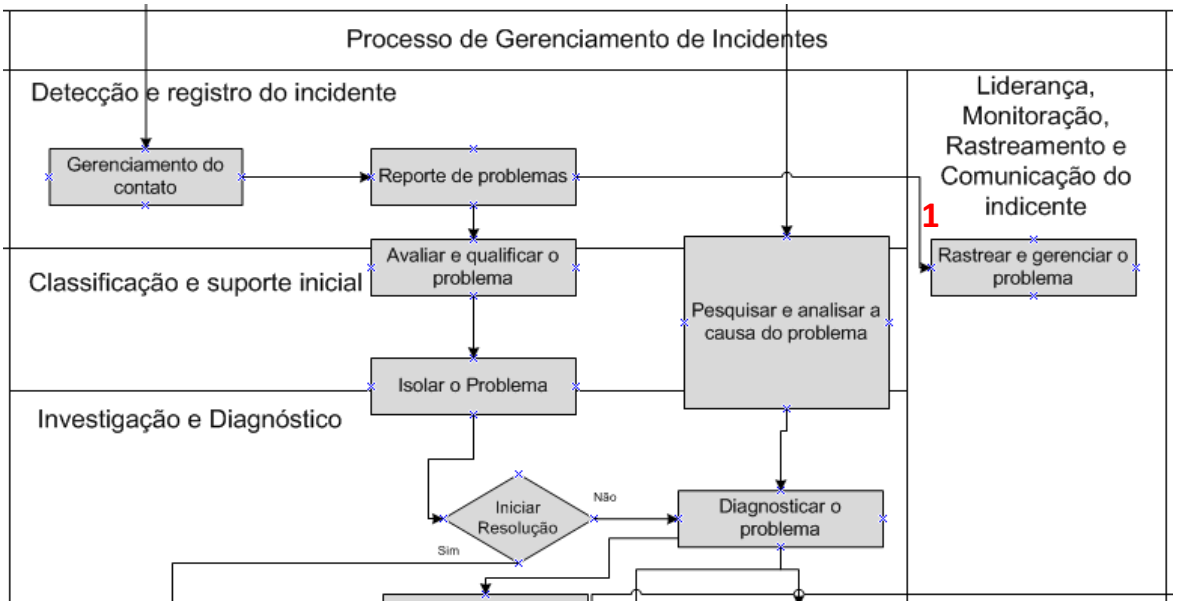

Figura 4 – Etapa de Investigação Liderança, Monitoração, Rastreamento e Comunicação do Incidente.

- **Causa Raiz** - A ação que é apresentada na sequência do relato do problema, como continuidade do fluxo no sentido vertical, é a qualificação e avaliação do problema, previsto na etapa de classificação e suporte inicial. Após esta etapa, propõe-se o isolamento do mesmo, como apontado na Figura 5, na etapa identificada pelo número 2. Questionou-se a coerência desta ação no fluxo apresentado, pois se entende que não seria possível efetuar o isolamento de um problema que não se conhece, ou que não tenha o elemento causador de tal evento identificado. Talvez fosse pertinente a tentativa de identificar se o problema poderia estar relacionado a um equipamento ou elemento nos sistemas de telecomunicações, e então tentar determinar a origem do problema ou isolar tal elemento do sistema. No entanto, mesmo nesta hipótese, para que tal ação pudesse ser realizada, o diagnóstico do problema precisaria ocorrer. Prosseguindo com a descrição do fluxo apresentado, visualiza-se que na etapa seguinte, propõe-se o início da resolução do problema em uma tomada de decisão, como indicado pelo número 3 apresentado Figura 5, e neste ponto ainda há o questionamento quanto à realização desta

ação sem que o diagnóstico, que é proposto na etapa seguinte e indicado na figura mediante o número 4, pudesse ser realizado.

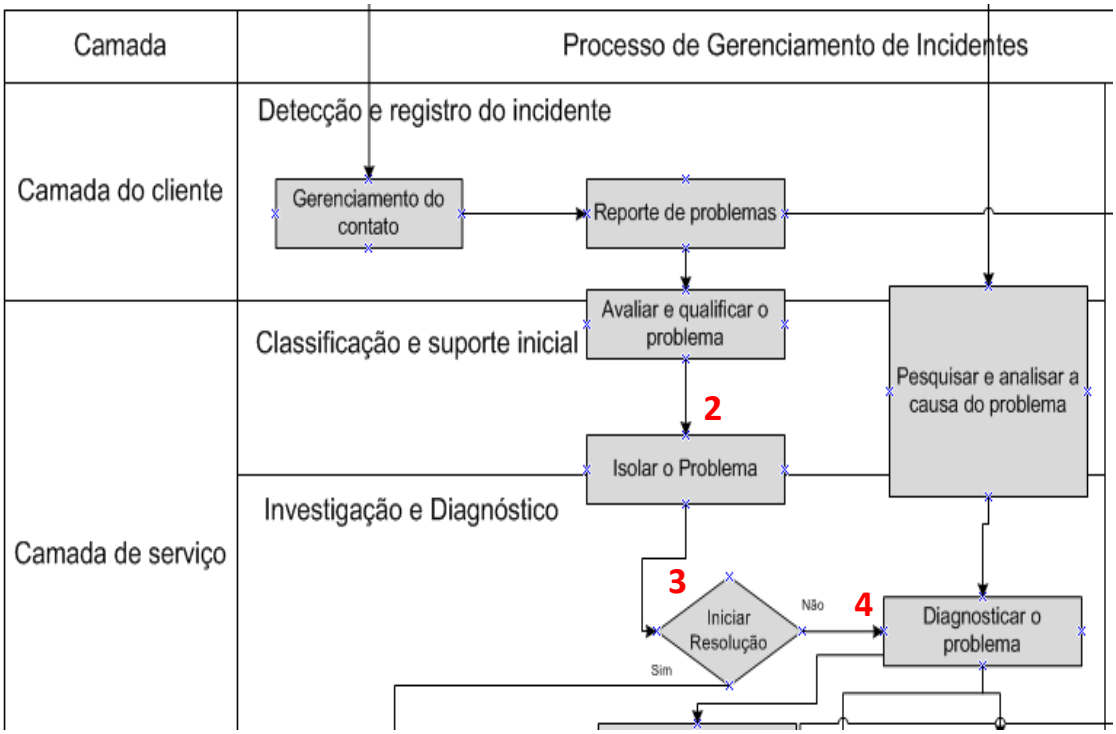

Figura 5 – Falhas identificadas no fluxo proposto por [1] para tratamento de incidentes – etapas de Detecção e registro do incidente, Classificação e suporte inicial e Investigação e diagnóstico.

- **Análise de impacto** - Após a etapa de diagnóstico do problema, é apresentada no fluxo a etapa de localização da causa do problema, a qual propõe que neste momento seja realizada a análise de impacto do serviço. Tal etapa é apresentada na Figura 6 e exibida no fluxo, mediante indicação realizada pelos números 5 e 6. Percebeu-se que tal análise ocorre somente depois de todo o processo de diagnóstico e localização da causa do problema ser concluído. Houve uma preocupação relevante com essa etapa, pois se o incidente estivesse relacionado com algo importante ou até mesmo essencial para o funcionamento do negócio de um cliente, ou houvesse um grau elevado de complexidade relacionado ao cenário problemático, certamente até que o diagnóstico fosse concluído, talvez a avaliação de impacto do serviço não se fizesse necessária. Certamente haveria uma crise relacionada ao cliente e o nível gerencial e executivo do

provedor de serviços já teria sido envolvido para acompanhar o problema, de maneira que o mesmo fosse solucionado com urgência.

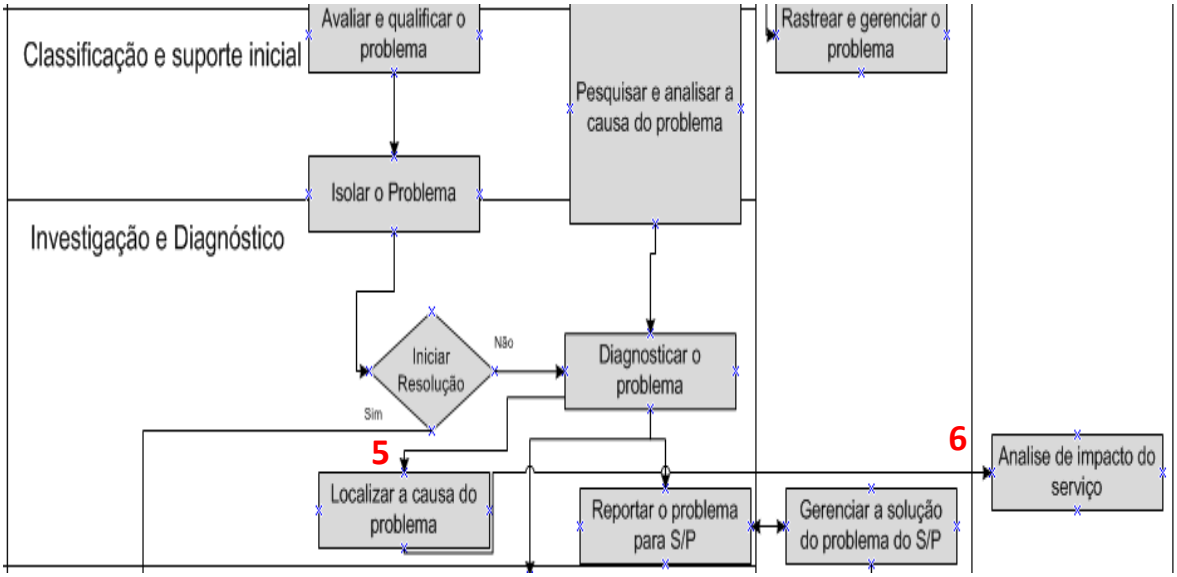

Figura 6 – Etapa de Investigação e diagnóstico – avaliação de impacto do serviço.

- **Priorização** – Questionou-se quanto à identificação do que é sensível para o funcionamento do negócio. Verificou-se que, em caso de um grande incidente, no qual fosse necessário priorizar o atendimento de um determinado sistema ou ambiente, a única forma disponível para tal ação seria a severidade do incidente, a qual está associada ao nível de serviço acordado com o cliente. Não se identificou na literatura um processo existente, no melhor do nosso conhecimento, para efetuar tal definição.
- **Base de conhecimento** – Analisando o diagrama proposto na Figura 3, não se identificou qualquer apontamento nas etapas apresentadas, que mencionasse identificar se o problema reportado pelo cliente era um problema já diagnosticado anteriormente. O ITIL propõe que todo o incidente que teve a sua causa raiz identificada, mediante o processo de análise da causa raiz, conhecido por sua sigla em inglês RCA (*Root Cause Analysis*), aplique uma solução definitiva para que o problema não ocorra novamente, e que essa solução seja documentada em uma base de conhecimento. Tal processo é contemplado no método proposto, indicado na Figura 7 pelo número 7. No entanto questionou-se a efetividade desse

processo, se não há no método qualquer consulta ao mesmo na etapa de diagnóstico, ou mesmo na avaliação e qualificação do problema.

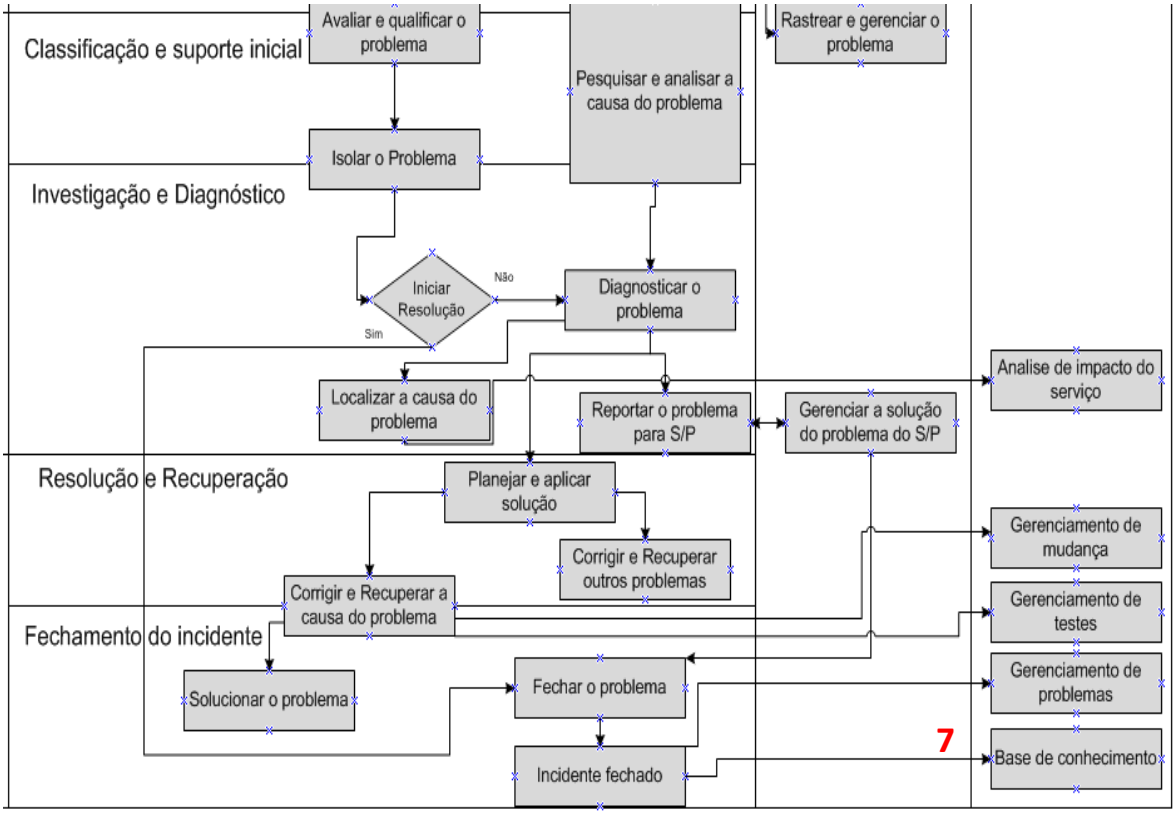

Figura 7 – Falha identificada na ausência de consulta a base de conhecimento.

3. O método

Neste capítulo, discute-se uma nova proposta para o diagnóstico e tratamento dos incidentes em sistemas de telecomunicações.

3.1. O método

Verificou-se a necessidade de desenvolver uma proposta que melhorasse os pontos identificados e relatados no capítulo anterior referente ao no modelo Z. A primeira sugestão ao modelo foi concebida ao analisar a convergência de diversos tipos de aplicações e funcionalidades para a rede, principalmente observando-se que nos dias atuais verificam-se sistemas de segurança que transmitem seus dados, contendo áudio e vídeo, através dos sistemas de comunicação bem como da Internet. Com uma infinidade de conteúdos compartilhando o mesmo meio de transmissão e a mesma infraestrutura, questionou-se sobre como definir o que deve ser tratado como prioridade no caso de uma indisponibilidade, seja ela de toda a comunicação da rede ou mesmo de um único sistema, quando todo incidente converge para uma única estrutura de atendimento. Certamente que em uma situação como a descrita anteriormente, seria necessário um critério de priorização, que considerasse o que é mais sensível à indisponibilidade. Nesta perspectiva, observaram-se vários métodos que se demonstraram eficientes para o tratamento e priorização de um determinado tipo de demanda, como a teoria de filas [39] ou ainda o diagrama de Voronoy [40], no entanto os dois modelos citados apresentam a priorização baseada em cálculos numéricos e estatísticos, e verificou-se que os mesmos nem sempre representam o sentimento e a necessidade do usuário ou a necessidade na perspectiva de negócio das empresas.

Identificou-se o segundo problema, que era determinar o que é crítico na perspectiva de uma empresa. Havia a necessidade de definir o que é um sistema crítico, pois no melhor do nosso conhecimento não se localizou tal definição na literatura. Adicionalmente, havia também a necessidade de correlacionar o que é crítico do ponto de vista de negócio ao que é crítico sob a perspectiva de infraestrutura de TI. Na ótica de TI não é incomum que a visão técnica esteja distante da visão relacionada ao negócio da empresa. Tal diferenciação muitas vezes torna complexo equalizar o que é sensível ao

negócio ao que está funcionando no ambiente de TI e rede. Verificou-se após um período de análise que os executivos de uma empresa possuem a visão daquilo que é indispensável para o funcionamento do negócio.

3.2. Mapeamento de Ambientes Críticos ao Negócio

Entendeu-se que o resultado dessa visão poderia ser aplicado ao parque de equipamentos da infraestrutura de TI e dos sistemas de Telecomunicações. Seria possível traduzir a visão executiva nos equipamentos que compõe a infraestrutura de TI e os sistemas de telecomunicações. Elaborou-se então um processo de estabelecimento de correlação entre o que é sensível e essencial para o funcionamento do negócio do cliente na perspectiva de gerenciamento e gestão empresarial, com o ambiente de tecnologia da informação no que diz respeito aos sistemas e equipamentos. O objetivo é obter uma visão de quais equipamentos e sistemas podem ocasionar sérios prejuízos à empresa, sejam eles financeiros, estratégicos, ou ainda que comprometam a imagem da companhia caso fiquem indisponíveis. Este processo foi nomeado Mapeamento de Ambientes Críticos ao Negócio (MACN). A Figura 8 demonstra o fluxo que o modelo propõe para o MACN.

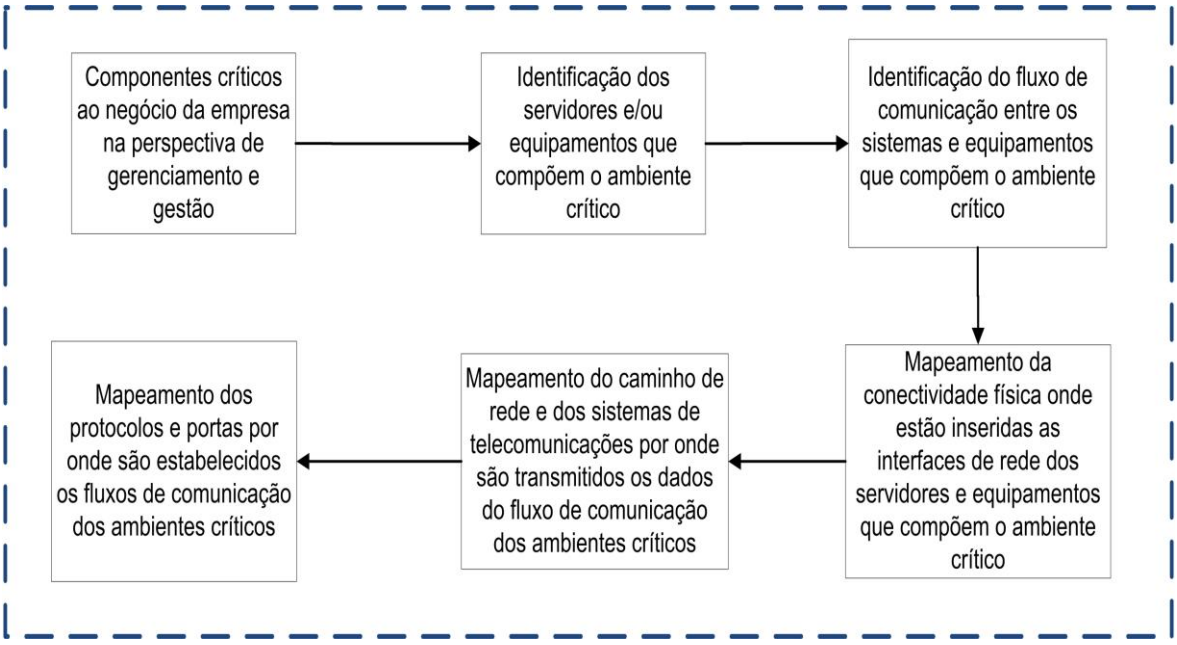

Figura 8 – Fluxo proposto para o MACN.

O fluxo para o MACN tem início na identificação dos componentes considerados críticos para o funcionamento do negócio de uma empresa, na perspectiva executiva, ou seja, que uma parada não planejada ocasionará problemas diversos para a empresa, e prejuízos financeiros também. Essa é a percepção que a visão da gestão empresarial possui relativa ao que é essencial para que a empresa continue com os seus objetivos estabelecidos e alcançáveis. Mediante esse mapeamento, torna-se possível definir o que é "crítico" na visão executiva de uma empresa. Uma vez definida o que é crítico na perspectiva do negócio, é necessário transpor essa visão executiva na infraestrutura de TI. Em outras palavras, significa identificar onde se encontram instalados os sistemas e elementos definidos pelos executivos como críticos, bem como por onde se comunicam. Sendo possível definir os elementos físicos que compõe o ambiente crítico, faz-se necessário identificar os fluxos de comunicação destes elementos com os demais equipamentos no sistema, mapeando cada interface e elementos por onde um fluxo de comunicação é estabelecido, e também por quais caminhos de rede e de telecomunicações os ambientes críticos se utilizam para a comunicação. Por fim, são mapeados todos os protocolos e portas lógicas que os fluxos de comunicação dos ambientes críticos são estabelecidos, provendo um mapeamento pleno dos elementos e da comunicação destes ambientes críticos e isto refletido à infraestrutura de TI e Telecomunicações. Desta forma, utilizando-se do fluxo proposto para o MACN, é possível identificar de forma rápida quais elementos ou sistemas devem ser priorizados em uma situação de falha ou indisponibilidade.

3.3. Acompanhamento Executivo de Incidentes Críticos

A partir desta realidade, verificou-se que uma vez mapeado aquilo que é crítico no ambiente dos clientes mediante uso do MACN, implementado no processo de esclarecimento e suporte inicial apresentado na Figura 12, é possível prover uma identificação de criticidade no início do incidente. Mediante tal identificação, seria possível também prover um alinhamento executivo na provedora de serviços. Entendeu-se que caso o incidente informado estivesse relacionado a algum sistema ou serviço crítico que foi mapeado através do MACN, haveria a necessidade de informar a gerência responsável pela operação de suporte, a respeito da abertura do incidente, informando a relação deste a ambientes sensíveis para o negócio da empresa, e o impacto que tal incidente estava ocasionando. Mediante essa comunicação, é possível um acompanhamento gerencial e executivo da provedora de serviços junto ao problema em tempo real, garantindo que todos os esforços necessários estarão concentrados para a

solução do problema no menor tempo possível. Tal processo também possibilita uma interação entre a estrutura de suporte e o cliente, demonstrando sinergia e cuidado com o ambiente gerenciado, bem como o direcionamento dos esforços no sentido de solucionar o mais rápido possível o problema. O processo descrito foi nomeado de AEIC, que significa Acompanhamento Executivo de Incidentes Críticos. A utilização deste processo na estrutura de suporte é exibida na Figura 12.

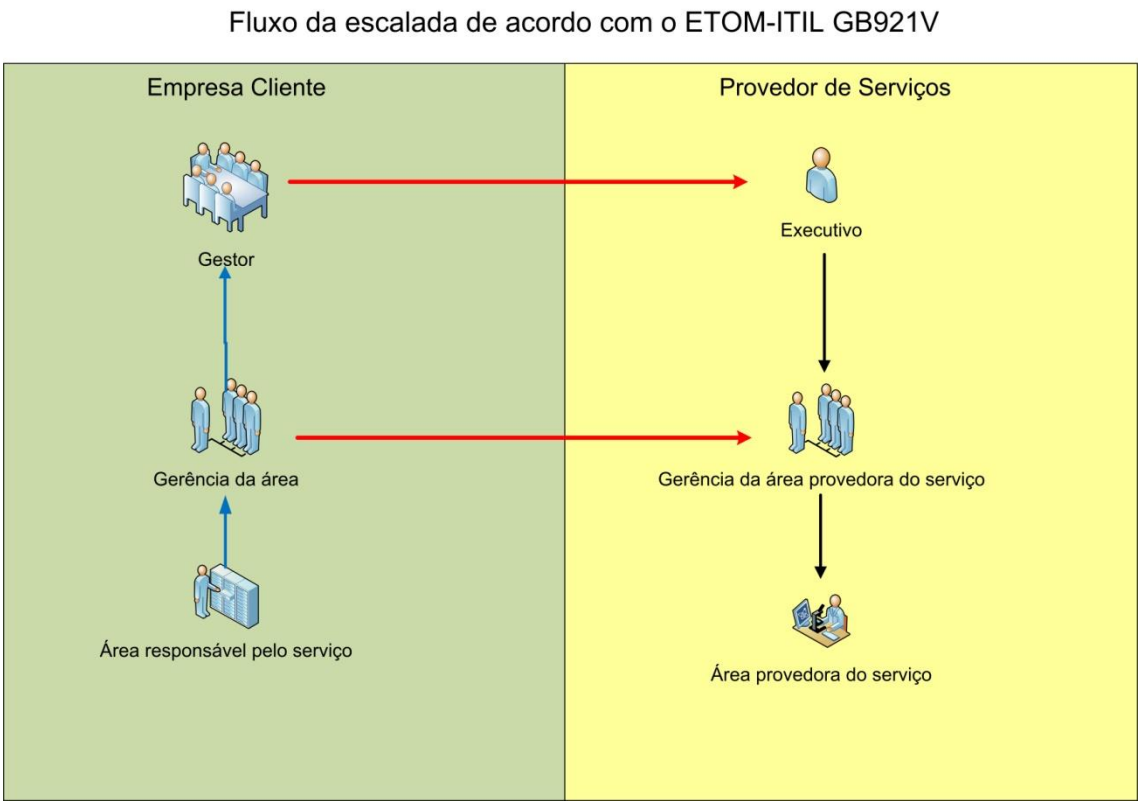

Figura 9 - Fluxo de escalada de acordo com GB921V

De acordo com [23] é previsto como parte do gerenciamento de problemas, o processo de escalonamento. A Figura 9 exibe este processo de escalada, que se inicia com a área responsável por um serviço prejudicado. Tal área após a abertura de um incidente junto à empresa provedora do serviço relatando o problema comunicará o mesmo ao nível gerencial, que por sua vez fará a interação com o nível gerencial da empresa provedora do serviço para cobrar a solução do problema. Também comunicará o problema ao nível de gestão, que envolverá os executivos da empresa provedora de serviço para que tomem as medidas necessárias para o pronto restabelecimento do mesmo.

O AEIC tem por objetivo prover uma pró-atividade gerencial e executiva. No momento em que um incidente é aberto pelo cliente, executa-se uma verificação para constatar se este está relacionado a algum sistema sensível ao negócio em questão previamente mapeado e classificado pelo MACN. Se o incidente não estiver impactando algo sensível ao negócio, o tratamento deverá seguir o fluxo normal de atendimento. Caso esteja mapeado como algo crítico, tão logo tenha ocorrido a qualificação do incidente, informa-se o nível executivo da operação a respeito do problema, permitindo ao gestor antecipar-se a escalada e interagir com o cliente, demonstrando atenção ao negócio e o cuidado com o cliente por parte da provedora de serviço. A Figura 10 apresenta esta pró-atividade prevista pelo AEIC, pois na identificação de um problema em um sistema crítico ao negócio, o responsável da área provedora do serviço informa ao gerente a respeito do problema, e este pode interagir com o cliente informando sobre o conhecimento do mesmo e quais ações estão sendo realizadas. O gerente da provedora de serviços pode então comunicar o nível executivo da mesma, com o mesmo intuito, e para que este verifique as ações estratégicas junto ao cliente.

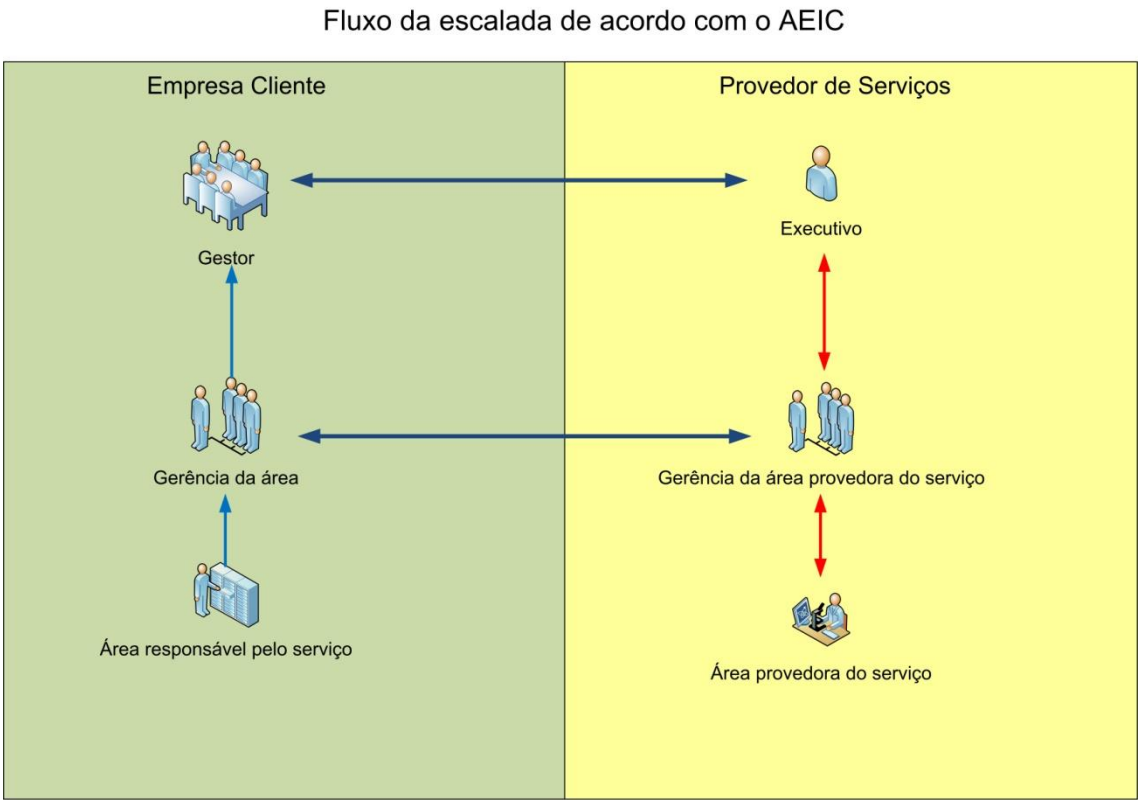

Figura 10 - Fluxo proposto pelo AIEC

3.4. Verificação de elementos de rede (LVR)

Como apresentado anteriormente, um incidente crítico reclamado pelo cliente, por meio de um tíquete aberto para a operação seguia o fluxo de incidentes em uma empresa e receberia um tratamento diferenciado sempre houvesse impacto em um sistema ou ambiente crítico para o negócio da empresa. Tal evento seria acompanhado pela linha gerencial e executiva da operação do provedor de serviços. No entanto, existia ainda uma dificuldade quanto à identificação do elemento causador do problema, caso não fosse localizado na base de conhecimento. Havia dúvidas a respeito de quais seriam as etapas a serem percorridas. O modelo Z apresentado por [1] apresenta uma etapa de diagnóstico, no entanto não há qualquer menção de como o mesmo é executado. O mesmo ocorreu quando recorremos aos métodos ITIL e eTOM, também pesquisados no presente trabalho. Verificou-se então na literatura alguma forma de verificação para diagnóstico de incidentes em sistemas de telecomunicações, mas no melhor do nosso conhecimento não se localizou nenhum método que pudesse rastrear tais incidentes de modo a identificar problemas.

Concebeu-se, então, um processo para verificar quais etapas devem ser executadas para rastrear e mitigar problemas nos sistemas de telecomunicações. A partir desse estudo foi elaborada uma Lista de Verificação de Rede denominada LVR, que constitui um processo que, apesar de sua concepção não ser inédita, ou seja, ser um processo já idealizado e comumente utilizado no processo de diagnóstico de problemas na rede, não se localizou documentação do mesmo em um método existente ou na literatura. Este processo foi criado com a finalidade de identificar as possíveis causas de problemas na transmissão de dados a partir dos equipamentos pertencentes à camada de rede, ou que se comunicam através da mesma. Tais itens são detalhados a seguir:

- **TAXA DE ERRO E COLISÕES**: Obtidos a partir dos indicadores disponíveis no gerenciador da interface dos equipamentos, principalmente elementos de rede como roteadores e *switches* gerenciáveis, contadores de erros nos pacotes de dados bem como colisões nas interfaces, que são fatores responsáveis, dentre outros problemas de comunicação, por lentidão.

- **TAXA DE TRANSMISSÃO E MODO DA INTERFACE**: É comum que os elementos possuam suas interfaces conectadas aos equipamentos de rede configurados com taxa e modo de transmissão automáticos. O problema desse tipo de configuração é que se o equipamento conectado ao elemento de rede for um *switch* ou um roteador, necessitará negociar parâmetros descritos com o

elemento a ele conectado, resultando em muitos casos em uma configuração que pode não ser apropriada para a conexão, ocasionando problemas.

- **INDICADORES DE DESCARTE DE PACOTES**: Mediante indicadores disponíveis nos equipamentos de rede como *switches* e roteadores é possível identificar se pacotes foram descartados. O descarte de pacotes ocorre quando não é possível transmitir, ou quando o tempo de validade de tal pacote expira. Isto ocorrendo, o dado será retransmitido, ocasionando atraso na comunicação que resultará em problema para o usuário.

- **GARGALO NO CAMINHO DE REDE ENTRE ORIGEM E DESTINO**: Eventualmente os caminhos de rede entre os elementos que se comunicam podem ter sua capacidade de transmissão de dados saturada, ocasionando retenções na transmissão de dados entre dois elementos que se comunicam pela rede. Quando isso ocorre, haverá um atraso na transmissão dos dados pelos elementos de rede que ocasionará lentidão na comunicação.

- **DIMENSIONAMENTO DE EQUIPAMENTOS DE REDE**: Em alguns casos um problema na transmissão dos dados entre origem e destino da comunicação pode ter como causa a escassez de recurso nos equipamentos de rede, resultando em lentidão na transmissão ou até indisponibilidade.

- **PROBLEMAS DE ROTEAMENTO DE PACOTES**: Empresas comumente possuem vários segmentos de rede que compõem o seu *backbone*. Devido à esse grande número de redes torna-se complexo e custoso cadastrar e controlar toda a comunicação e alteração dessas redes nos equipamentos responsáveis por estabelecer a comunicação entre elas. Para minimizar tal controle, existem protocolos de roteamento dinâmicos, que são responsáveis por estabelecer a conectividade lógica entre todas as redes de forma automática, pois todo o processo é realizado mediante protocolos de roteamento. O problema é que, por ser um processo automático, e devido à grande quantidade de segmentos de rede que pode existir em determinados *backbones* além da complexidade da rede, podem ocorrer falhas no funcionamento e na estrutura de tais protocolos. Tais falhas podem ocasionar problemas como *loops* de roteamento dentre outros, que irão ocasionar lentidão e até mesmo indisponibilidade da comunicação.

4. Uma nova proposta para gerenciamento de incidentes

Para solucionar as falhas identificadas no modelo Z, foi criada uma nova proposta de fluxo, com a inclusão dos processos descritos. Esta proposta foi nominada de MALF, que é a sigla de MACN, AEIC, LVR e Fluxo. Sua composição é exibida na Figura 11.

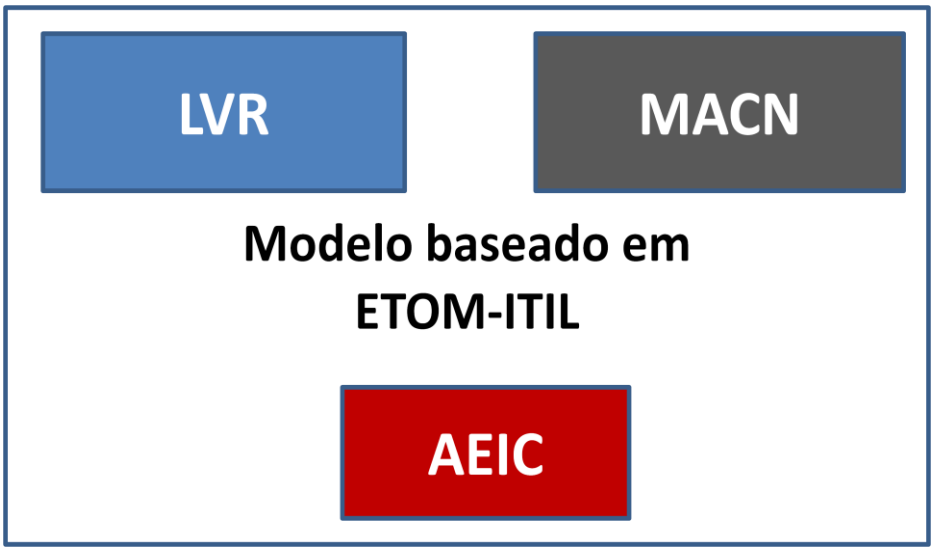

Figura 11 – Modelo baseado no ETOM-ITIL acrescido dos processos MACN, AEIC e LVR, nomeado de método MALF

O método MALF é composto de um modelo baseado em eTOM-ITIL, com a inclusão dos processos MACN, AEIC e LVR, descritos nas seções anteriores. A seguir são apresentadas cada uma das deficiências apontadas no modelo Z e que são corrigidas no método MALF.

- **Priorização** - Quando há a manifestação de algum cliente sobre uma falha ou um incidente, é necessário que ocorra uma qualificação esclarecimentos considerando que tal evento pode ser classificado de duas formas: uma solicitação de serviços ou um incidente. Compreendeu-se que uma solicitação de serviço normalmente está associada à prática

de alguma nova funcionalidade ou a alteração de algo que já está em funcionamento. Seja qual for a solicitação, entendeu-se que em uma situação normal tais solicitações compreendem alterações que possuem um tempo e um nível baixo de urgência e que por esta razão podem seguir o fluxo de atendimento normal de uma operação de rede. Todavia quando o evento manifestado pelo cliente está relacionado à indisponibilidade de um elemento ou do sistema de telecomunicações, poderá haver uma grande urgência para que o mesmo seja solucionado, pois certamente haverá algum impacto no negócio da empresa como consequência da indisponibilidade relatada. A aplicação do MACN provê essa priorização, uma vez que na etapa inicial, um incidente será classificado como crítico se estiver relacionado a algum equipamento ou sistema mapeado pelo MACN. Mediante esse entendimento, estruturou-se a etapa inicial de atendimento para que classificasse os eventos em requisições e incidentes na qualificação inicial, e em caso do evento estar classificado como incidente, se o mesmo era classificado como crítico, ou não. Tal estruturação é apresentada na Figura 12.

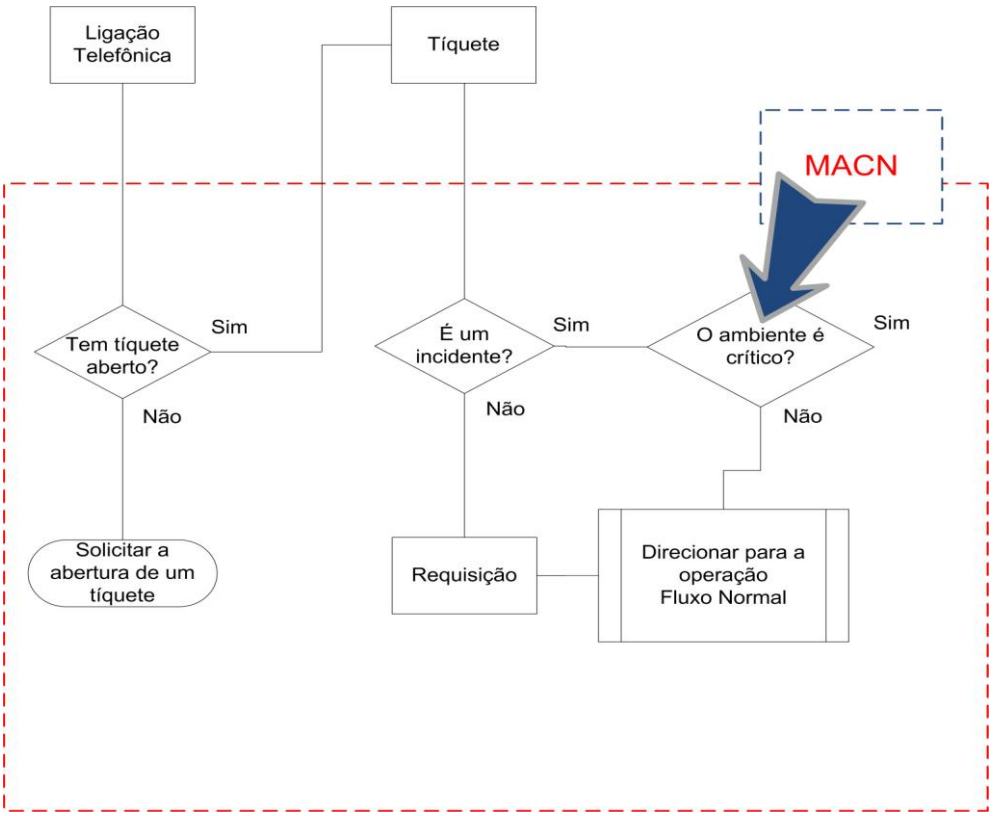

Figura 12 – Camada de Serviço – esclarecimentos e suporte inicial

Essa estruturação foi sobreposta ao contexto de camadas contido no modelo Z proposto por [1], apresentado na Figura 3. A camada apresentada no método MALF corresponde à camada de serviço, em sua primeira etapa que é a fase de esclarecimentos e suporte inicial.

- **Análise de Impacto** - Verificou-se que, mediante a prática do MACN, é possível no momento da abertura e qualificação de um incidente, determinar se este afeta algo crítico na perspectiva de negócio da empresa. Além disso, é possível estabelecer uma correlação com indicadores executivos, com o objetivo de dimensionar riscos, tanto financeiros como de imagem da reclamante, e na visão da operação poder distinguir este incidente dos demais e definir a sua prioridade em comparação a um incidente cuja criticidade é mais baixa. O mapeamento proposto, quando aplicado sob a visão de uma provedora de serviços de Telecomunicações, possibilita uma visibilidade do impacto no funcionamento do negócio do cliente, permitindo que o time técnico que atuará na recuperação do sistema ou serviço prestado tenha o senso correto de urgência para o restabelecimento dos serviços.
- **Interação com o cliente** – A incorporação do AEIC ao método MALF proporciona a interação com o cliente para o gerenciamento de crises provenientes do impacto ocasionado pela indisponibilidade ou falha no sistema de telecomunicações. Incorporou-se este método ao fluxo de incidentes na camada de serviço correspondente a etapa de liderança do incidente, na qual estão previstas as atividades de monitoração, rastreamento e comunicação. A camada transformada é apresentada no diagrama da Figura 13:

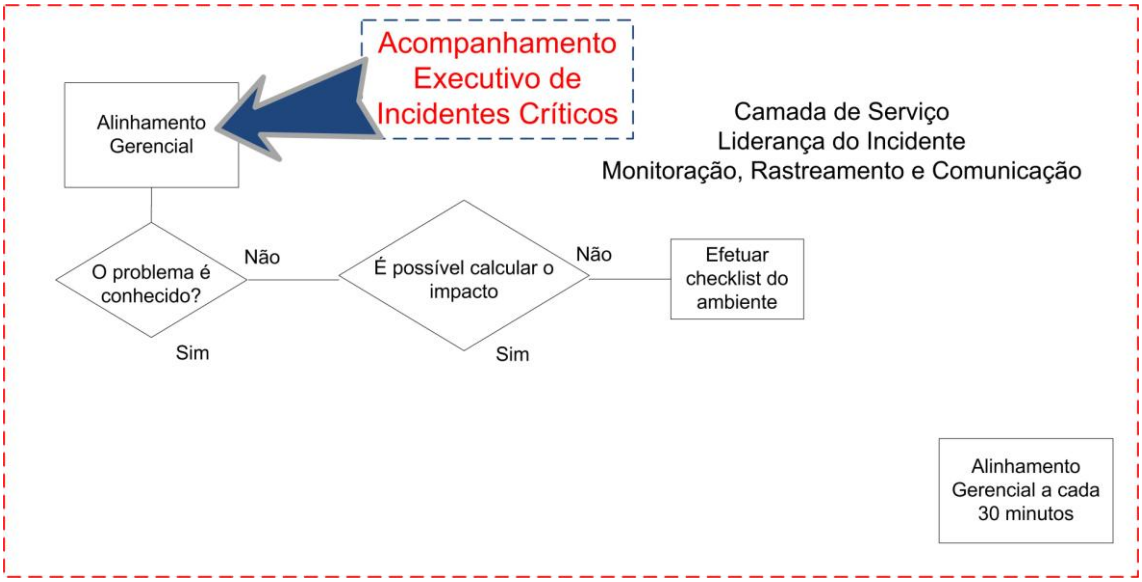

Figura 13 – Camada de Serviço – Monitoramento, Rastreamento e Comunicação

De acordo com o novo fluxo, assim que um incidente é classificado como crítico, de acordo com o MACN há o acionamento do nível executivo da operação para informar que um ambiente associado a um grande impacto está sendo afetado.

- **Base de Conhecimento** – Foi inserida, também, na camada descrita na Figura 13, a consulta à base de conhecimento utilizada para armazenamento de informações resultantes do processo de análise da causa raiz de problemas, previsto no ITIL. Essa base é utilizada na estrutura de suporte com o objetivo de identificar se o incidente informado já havia ocorrido anteriormente. Caso o incidente seja recorrente, é necessário identificar se são aplicáveis as mesmas medidas para a solução do problema, e quais são estas medidas. Este é um processo que no modelo Z não faz parte da camada de rastreamento do incidente. Entendeu-se ser útil tal consulta, mesmo em incidentes críticos, pois haveria um ganho importante de tempo no processo de diagnóstico do problema caso o mesmo já tivesse sido diagnosticado anteriormente.
- **Rastreamento do Problema** – A LVR foi acrescentada também ao fluxo do método MALF, na camada de serviço correspondente à etapa de nome liderança do incidente, na qual estão previstas as atividades de monitoração, rastreamento e comunicação. Seu objetivo é prover a rastreabilidade do problema, bem como o seu diagnóstico, mediante as

verificações que o processo propõe. Sua aplicação no método MALF é exibida na Figura 14.

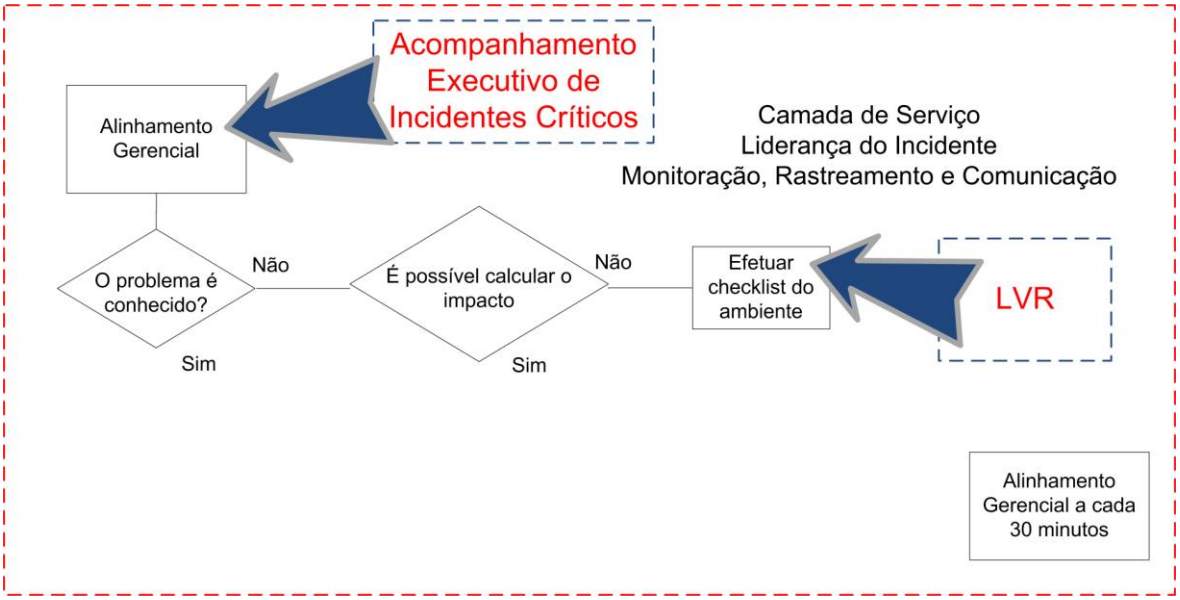

Figura 14 – Camada de Serviço – Monitoramento, Rastreamento e Comunicação com a implementação da LVR

- **Causa Raiz** – Com a incorporação da LVR ao fluxo de atendimento, foi possível estabelecer um método para o diagnóstico e o rastreamento da causa raiz de um incidente ocasionado nos sistemas de telecomunicações.

No entanto, ainda havia uma pendência na estruturação proposta, relativa à possibilidade de causa do problema por um elemento externo, ou ainda de falhas nas verificações. Havia dúvidas de como seria finalizado o diagnóstico, bem como quais procedimentos seriam adotados para garantir que o problema fosse localizado e resolvido. Ampliando-se a discussão em uma visão sistêmica que englobe também as redes e localidades remotas mediante a WAN (Wide Area Network), a complexidade para o diagnóstico do problema pode tornar-se ainda maior, uma vez que outras variáveis como problemas e falhas em circuitos de comunicação, problemas nos protocolos que fornecem a conectividade lógica, erros operacionais ocasionados em elementos físicos ou lógicos, dentre outros, podem ocasionar a falha ou indisponibilidade da comunicação.

Propôs-se um fluxo de verificação ao método MALF, que foi contraposto ao modelo Z apresentado por [1]. Tal estruturação mostrou abranger todos os aspectos necessários para o diagnóstico e tratamento de incidentes em sistemas de

telecomunicações. A Figura 15 apresenta tal método proposto, aplicado à operação de uma provedora de serviços:

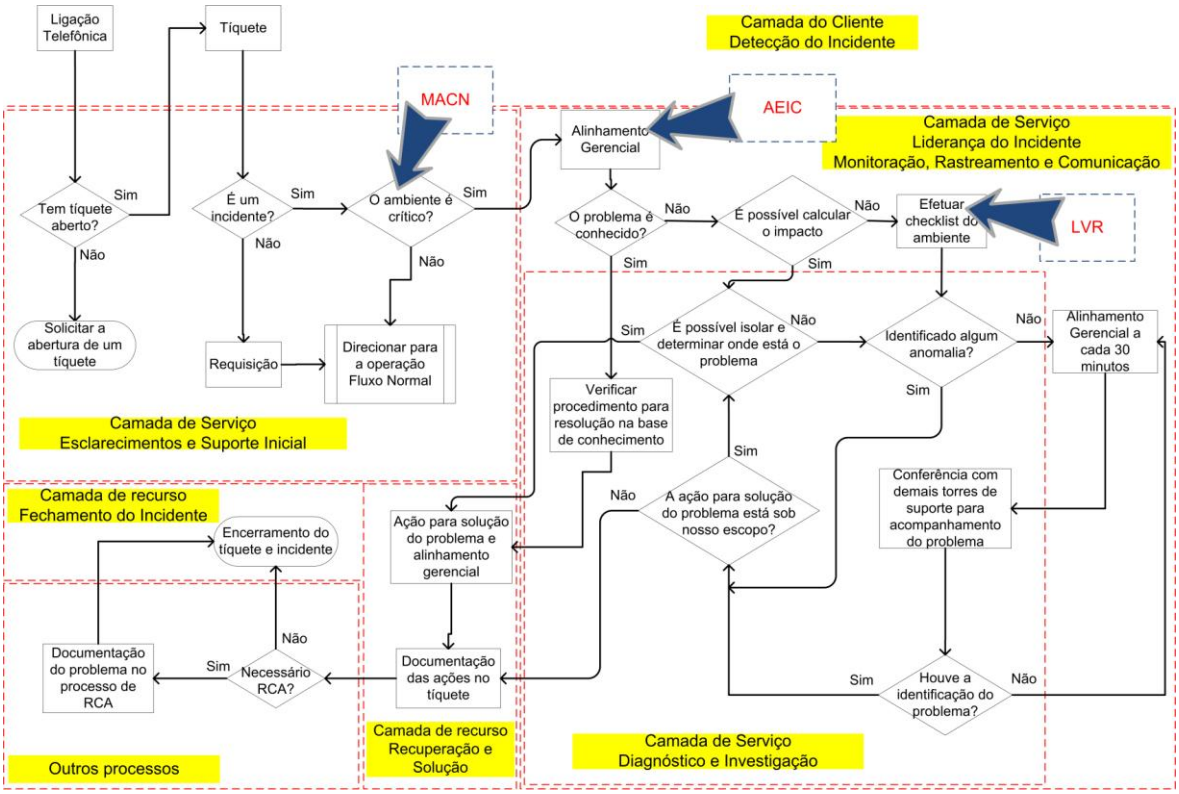

Figura 15- Proposta para estrutura e fluxo de atendimento de uma operação.

Nesta proposta, a camada do cliente é composta pela abertura de um chamado relatando o problema. Mediante o mesmo, o incidente deverá ser analisado pela operação responsável pelo atendimento inicial, o qual é realizado na etapa seguinte:

- **Camada de Serviço** – Compreende a etapa de esclarecimentos e suporte inicial na qual ocorre o processo de qualificação do chamado, analisando se o *tíquete* contempla uma requisição ou se constitui um incidente. Esta etapa contempla adicionalmente se comparada com a proposta apresentada na figura 5, a identificação do tipo de tíquete no que tange a criticidade. Se o incidente não está relacionado a um problema crítico, então o atendimento deve ser realizado pela operação, seguindo o fluxo normal de atendimento. Incidentes qualificados como críticos devem ser imediatamente comunicados para o nível gerencial, para que possa ser realizado o acompanhamento executivo previsto no processo AEIC. Após a comunicação gerencial verifica-se a base de conhecimento, que é parte do

modelo proposto no método ITIL, a fim de identificar se o problema já foi diagnosticado em outros momentos ou se o incidente é desconhecido. Caso o incidente seja reincidente, isto é, já houve uma ocorrência e diagnóstico anterior, verifica-se o método para resolução e aplicam-se as etapas descritas na “Camada de Recurso”. Tratando-se de um problema ainda não diagnosticado, verifica-se a possibilidade de identificar o impacto. Caso seja possível a identificação do impacto, então há a tentativa de isolar e determinar onde está o problema. Sendo possível determinar o problema, aplica-se a resolução do mesmo. Na impossibilidade de calcular o impacto, então se determina a execução das verificações previstas na LVR. Se mediante esta execução for possível identificar alguma anomalia, verifica-se a propriedade da ação para solução da anomalia. Caso seja da operação descrita na proposta, então se aplica o isolamento do problema, se possível, e aplica-se o mesmo fluxo de decisão na determinação do problema. Caso a ação para solução do problema não esteja no escopo da operação descrita na proposta, documenta-se o tíquete e aplica-se o procedimento para encerramento do mesmo, informando o cliente das ações tomadas. Se mesmo com a execução da LVR não for possível identificar alguma anomalia, realiza-se um novo reporte ao gerente da operação, e é realizada uma conferência telefônica com os demais times de apoio para acompanhamento e identificação do problema. Esse processo é realizado a cada 30 minutos até a identificação de alguma anomalia ou da causa do problema.

- **Camada de Recurso** – Esta camada compreende as ações para solução do problema, prevendo um informe gerencial de tais ações, e a devida documentação no tíquete de problema, bem como aplicação dos procedimentos para encerramento do incidente.
- **Outros processos** – Estão previstas nessa camada a etapa de qualificação e descrição da causa raiz do incidente, e a solução definitiva, ou sua investigação, caso necessário, conforme processo ITIL. De acordo com o processo de identificação da causa raiz ocorre o registro da mesma na base de conhecimento, para que em eventos futuros as informações sobre o problema possam auxiliar o diagnóstico e tratamento do incidente.

5. Aplicação do Método

Neste capítulo apresenta-se a aplicação dos processos criados a um dos clientes de uma empresa provedora de serviços de gerenciamento de redes e telecomunicações. Descreve-se o sistema experimental e a aplicação do método proposto.

5.1. Descrição do cenário utilizado para a validação

Para proceder à validação do método, utilizou-se o provimento dos serviços de gerenciamento de rede e sistemas de telecomunicações de uma empresa global para 68 empresas clientes nacionais de diversos tamanhos e objetivos de negócio. Selecionou-se um dos clientes da provedora de serviços para a prática e validação da proposta. Tal cliente selecionado é líder em seu setor, detendo 80% do mercado mundial na área em que atua, e com representatividade em diversos países. O escopo de atuação da provedora de serviços neste cliente é o gerenciamento de redes e segurança, não sendo responsabilidade da mesma os links de comunicação entre as localidades do cliente.

Selecionou-se a aplicação mais importante deste cliente para validar o modelo e os processos propostos, denominada *Desktop* Virtual (DV). Esta é uma aplicação na qual está o ambiente de trabalho do usuário (*desktop*), cuja indisponibilidade afeta diretamente os negócios do cliente (vendas, produção, compras, logística). Utilizam-se dessa estrutura aproximadamente 32 mil usuários nominais, sendo que destes, aproximadamente 11 mil são acessos simultâneos. Tal empresa possui diversas localidades em âmbito nacional, sendo que todas elas utilizam a estrutura de DV, que está instalada em uma estrutura composta por mais de 200 servidores localizados em um *Data Center* (DC) centralizado. O acesso das localidades até o DC é feito mediante a utilização de diversos circuitos de comunicação, os quais provêem aos usuários de cada localidade a área de trabalho virtual, sem a qual ele não consegue desenvolver suas atividades, uma vez que apenas 10% dos equipamentos do parque de TI que atendem os usuários são computadores físicos. Os demais 90% são equipamentos denominados *ThinClient*, que são terminais com monitor, teclado e mouse, e uma caixa com placa de rede e o sistema de inicialização, o qual busca a imagem da área de trabalho nos servidores remotos [41][42]. A indisponibilidade de um circuito de comunicação, ou ainda dos servidores localizados no DC representa a parada total da produção e prestação de

serviços de uma localidade e, consequentemente, severos prejuízos para a mesma. É importante complementar que, como parte do ambiente de DV estão os serviços que os usuários se utilizam, como e-mail, navegação de internet ou acesso a algumas aplicações WEB, que são consideradas parte da solução do DV. Em outras palavras, qualquer problema ou indisponibilidade em uma ou algumas dessas ferramentas também afeta a disponibilidade do ambiente DV.

O cliente utilizado para validar o método foi analisado por um período de seis meses, compreendendo os meses de Janeiro a Junho do ano de 2012. Tal cliente relatou problemas mediante a abertura de 31 tíquetes de reclamação, sendo que deste total, quatro incidentes foram classificados como incidentes com severidade 1, sendo esta a severidade que necessitava do menor tempo para o atendimento e solução do problema, de acordo com o nível de serviço estabelecido com o cliente. Os dados dos tíquetes relatados neste período são apresentados a seguir:

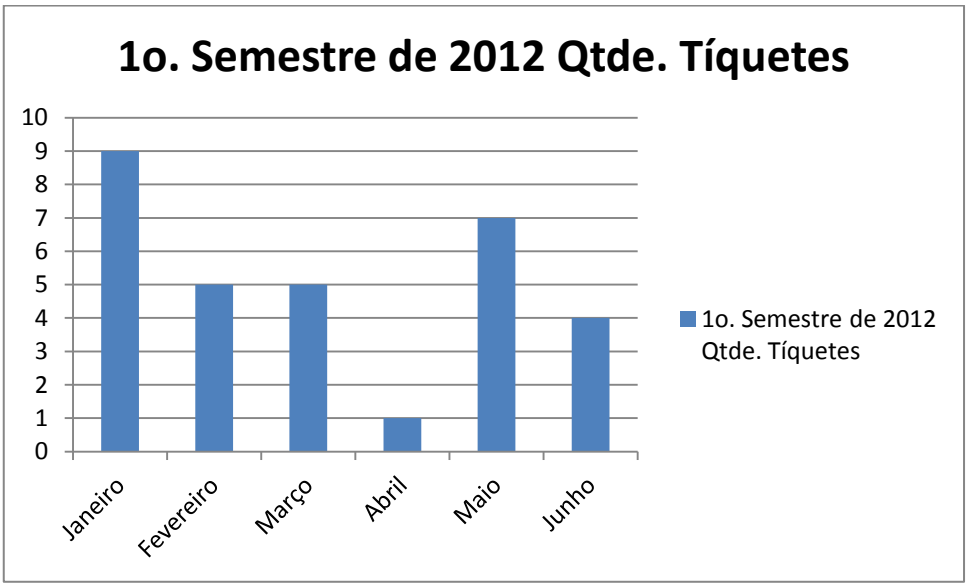

Figura 16 - Volume mensal de tíquetes abertos pelo cliente em 2012

Verificaram-se os dados coletados nos tíquetes antes da prática do método proposto no presente trabalho. Para tal análise, foi estabelecida a utilização apenas de incidentes classificados como críticos. No entanto, antes da prática do MACN, não havia a definição de incidentes críticos, pois não existia uma forma de classificá-los como tal. Definiu-se então utilizar a severidade mais restritiva do sistema de tíquetes, que é a forma que o *Help Desk* possuía para informar à operação sobre a urgência do atendimento. Neste caso, utilizou-se a severidade 1. Verificou-se nos tíquetes

observados que o atendimento do incidente nem sempre ocorria de forma rápida, bem como se observou demora no diagnóstico e tratamento do mesmo.

Efetuou-se a classificação de tais incidentes por categoria de problema. Os dados de tal categorização são exibidos a seguir:

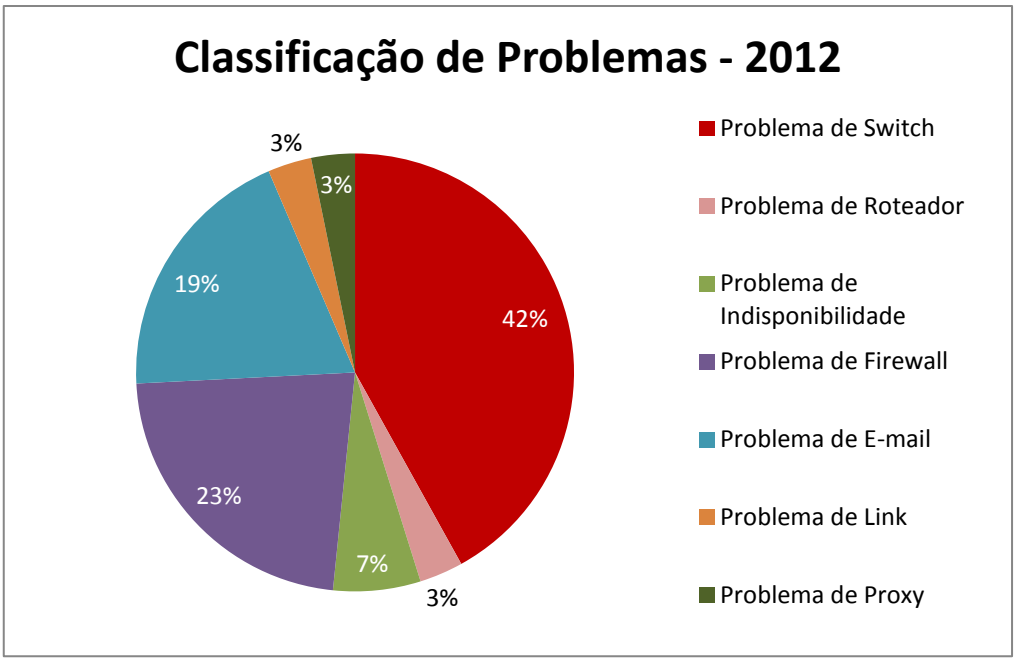

Figura 17 - Classificação dos tipos de problemas - 2012

Verificou-se que do total de incidentes abertos, 42% eram incidentes classificados como “Problema de Switch”. Tais incidentes podem ocorrer devido a erros em interfaces ocasionadas por falhas na infraestrutura física, excesso de tráfego nas interfaces, falhas na configuração de taxa ou modo de transmissão nas interfaces de rede de servidores. Os incidentes abertos para tais dados eram constantemente analisados individualmente, não sendo possível identificar as causas de tais eventos na maioria dos casos, como pode ser observado nos dados dos eventos apresentados a seguir. Algumas informações foram ocultadas por razões de confidencialidade.

Evento	Detalhes
1	**Descrição**: XXXX: 5020A1 esta apresentando taxa de erros ou colisões acima do aceitável em alguma(s) interface(s). (Ex: LANErrorsIn na Ethernet121/1/42 (- hostname = 5020A1 Class: DS_Service_Alarm **Data e hora de abertura**: 25/01/2012 10h25min **Data e hora de encerramento**: 25/01/2012 12h01min **Tempo de atendimento**: 01h36min **Solução**: Não houve incremento de erros no período monitorado. Possível frame inválido gerado pelo robot. 5020A1 sh int Eth121/1/42 Ethernet121/1/42 is up Hardware: 100/1000 Ethernet, address: 588d.0916.212b (bia 588d.0916.212b) Description: Robot (n/s 78a2484) MTU 1500 bytes, BW 100000 Kbit, DLY 10 usec, reliability 255/255, txload 1/255, rxload 1/255 Encapsulation ARPA Port mode is access full-duplex, 100 Mb/s Beacon is turned off Input flow-control is

Tabela 1- Evento classificado como "problema de switch" - Exemplo 1

Evento	Detalhes
2	**Descrição**: XXXX: 5020A1 esta apresentando taxa de erros ou colisões acima do aceitável em alguma(s) interface(s). (Ex: LANErrorsIn na Ethernet113/1/34 (- hostname = 5020B1 Class: DS_Service_Alarm **Data e hora de abertura**: 13/01/2012 13h07min **Data e hora de encerramento**: 13/01/2012 14h15min **Tempo de atendimento**: 01h08min **Solução**: Não houve incremento de erros no período monitorado. Possível frame inválido gerado pelo robot. 5020A1 sh int Ethernet113/1/34 is up Hardware: 100/1000 Ethernet, address: 588d.0854.7a5c (bia 588d.0854.7a5c) Description: Robot (n/s 78a2484) MTU 1500 bytes, BW 100000 Kbit, DLY 10 usec, reliability 255/255, txload 1/255, rxload 1/255 Encapsulation ARPA Port mode is access full-duplex, 100 Mb/s Beacon is turned off Input flow-control is

Tabela 2 - Evento classificado como "Problema de Switch" - Exemplo2

Evento	Detalhes
3	**Descrição**: XXXX: 5020A1 esta apresentando utilização acima do aceitável na interface Ethernet101/1/25 (- hostname = 5020A1) **Data e hora de abertura**: 18/02/2012 15h23min **Data e hora de encerramento**: 18/02/2012 17h45min **Tempo de atendimento**: 02h22min **Solução**: Não foi identificada alta utilização no período monitorado. Possível frame inválido gerado pelo robot. 5020A1 sh int Ethernet101/1/25 is up Hardware: 1000/1000 Ethernet, address: 588d.00dc.35ab (bia 588d.00dc.35ab) Description: Robot (n/s 78a2484) MTU 1500 bytes, BW 100000 Kbit, DLY 10 usec, reliability 255/255, txload 189/255, rxload 156/255 Encapsulation ARPA Port mode is access full-duplex, 1000 Mb/s Beacon is turned off Input flow-control is

Tabela 3 - Evento classificado como "Problema de Switch" - Exemplo 3

Para os casos verificados nos chamados, a causa dos problemas não pôde ser verificada, pois no momento que se executaram os testes não havia mais o problema, não sendo possível localizar sua causa. O mesmo se aplica ao incidente identificado como “Problema de Roteador” e “Problema de Link”, pois em ambos os casos os problemas eram semelhantes, bem como sua solução. Tais problemas são apresentados a seguir:

Evento	Detalhes
4	**Descrição**: XXXXXX 11 XXXXX LOCALIDADE xxxxxx SOLICITA VERIFICACAO DO LINK DA LAN DO DATACENTER, POIS DURANTE A TARDE HOUVE UM PROBLEMA DE LINK COM A EMBRATEL E QUER QUE VERIFIQUEM SE ESTA AFETANDO O DATACENTER, POIS O MESMO LINK FAZ LIGACAO COM A REDE GLOBAL DA XXXX. **Data e hora de abertura**: 16/05/2012 18h48min **Data e hora de encerramento**: 16/05/2012 22h49min **Tempo de atendimento**: 04h01min **Solução**: Não identificado o problema no ambiente

Tabela 4 - Evento classificado como "Problema de Link" - Exemplo 4

Evento	Detalhes
5	**Descrição**: Unix - Problemas de Lentidão no Servidor Nome: XXXXXX Telefone: XXXXX E-mail: XXX@XXXX Hostname do Servidor UNIX: XXXXXX Descricao do Problema: Por favor liberar os ip de origem 192.168.5.8 e 192.168.5.7 para acesso aos servidores e ferramentas de trabalho referentes ao servicos prestados pela XXXX. O log a seguir mostra o problema que esta ocorrendo: c:\>tracert -d 158.98.176.80 Tracing route to 158.98.176.80 over a maximum of 30 hop **Data e hora de abertura**: 17/05/2012 16:07 **Data e hora de encerramento**: 17/05/2012 20:51 **Tempo de atendimento**: 04h46min **Solução**: Descrição do incidente: Solicitação de verificação em firewall. Ações tomadas: Monitoramos o fluxo no ambiente e notamos que a comunicação ocorre normalmente: 19:55:05.715257 192.168.5.8.21932 > 158.98.176.80.http: . ack 13801 win 65535 (DF) 19:55:05.717237 158.98.176.80.http > 192.168.5.8.21932: . 22081:23461(1380) ack 589 win 64947 (DF) 19:55:05.717354 158.98.176.80.http > 192.168.5.8.21932: . 23461:24841(1380) ack 589 win 64947 (DF) 19:55:06.022155 192.168.5.8.21932 >

Tabela 5 - Evento classificado como "Problema de Router" - Exemplo 5

Quantos aos eventos classificados como “Problemas de Proxy”, “Problemas de Firewall”, e “Problemas de E-mail”, os mesmos não são apresentados, por tratarem especificamente de problemas decorrentes da falta de implementação de fluxo não mapeado previamente à sua utilização, associados a falta de conhecimento dos processos de comunicação utilizados pelos sistemas que compõem o DV. Em outras palavras, os incidentes foram ocasionados por falta do conhecimento da necessidade da aplicação de regras nos elementos descritos para que a solução pudesse funcionar corretamente.

5.2. Eventos críticos

Neste parágrafo, são exibidos os casos que demonstram problemas relatados pelo cliente, que estão relacionados ao ambiente DV, e foram classificados como severidade 1, pois não havia outra maneira de demonstrar a urgência no atendimento do mesmo, bem como de priorizar seu atendimento.

Evento	Detalhes
6	**Descrição**: Indisponibilidade do acesso ao DV via Web **Data e hora de abertura**: 26/02/2012 12h31min **Data e hora de encerramento**: 26/02/2012 14h19min **Tempo de atendimento**: 01h48min **Solução**: Em conferência realizada com outras áreas, foi verificado que o ambiente de redes esta OK. O Acesso externo à página do DV está OK, sem lentidão e perda de pacotes, segue: (anexas evidências do teste)

Tabela 6 – Eventos coletados no ano de 2012, relacionados ao ambiente de DV

No evento apresentado, nota-se que foi identificado pelo cliente um evento que ocasionava indisponibilidade de acesso ao ambiente DV via Web. O evento foi relatado pelo cliente às 12h31min, sendo que, segundo a informação inserida no tíquete pelo analista que efetuou o atendimento, o ambiente não apresentava problemas na perspectiva técnica. O tempo de atendimento do incidente foi de 01h48min e não foi localizada a causa do problema.

Evento	Detalhes
7	**Descrição**: DV - Lentidão no Aplicativo Dados do solicitante Nome: XXXXX Telefone: XXXXX Email: XXXXX Empresa: XXXX: Login do Usuário: XXXX Servidor: * Horário em que a lentidão iniciou: 18h27min Descrição: Indisponibilidade de acesso ao site XXXX. Cliente informa que nao consegue acessar o DV via WA **Data e hora de abertura**: 08/04/2012 18h28min **Data e hora de encerramento**: 08/04/2012 22h48min **Tempo de atendimento**: 04h20min **Solução**: Descrição do incidente: Problemas de acesso externo a website da XXX. Ações tomadas: Verificado que a resolucao DNS para o IP ocorre normalmente: [server]$ nslookup XXX.XXX.com.br Note: nslookup is deprecated and may be removed from future releases. Consider using the `dig or `host programs instead. Run nslookup with the `-sil[ent] option to prevent this message from appearing. Server: 192.168.10.4 Address: 192.168.10.4#53 Name:

Tabela 7 – Eventos coletados no ano de 2012, relacionados ao ambiente de DV

Neste evento, identificou-se pelo cliente uma indisponibilidade de acesso ao ambiente DV via Web. O evento foi relatado pelo cliente às 18h28min. Verificou-se que o problema estava relacionado à resolução de nomes. No entanto, após 4 horas, a causa do problema não foi identificada e o ambiente foi restabelecido sem a identificação da causa raiz.

Para todos os eventos exibidos, utilizou-se o fluxo da operação, descrito na Figura 18 para o tratamento do incidente.

5.3. Estrutura da operação na provedora de serviços

Nesta sessão, apresenta-se a figura desenvolvida neste trabalho para mostrar o fluxo de atendimento de um incidente na operação de gerenciamento de incidentes da provedora de serviços de gerenciamento de redes de computadores e sistemas de telecomunicações. O diagrama inicial da operação é apresentado na Figura 18.

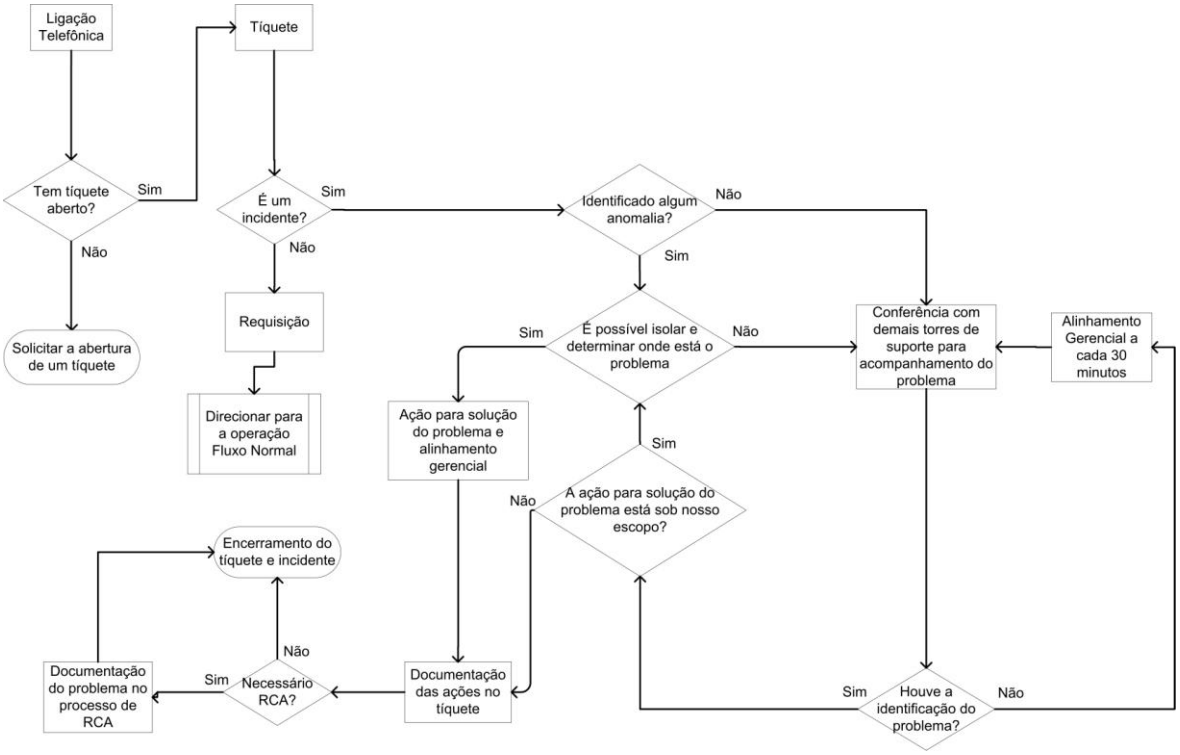

Figura 18 – Fluxo de atendimento da operação na provedora de serviços.

De acordo com o fluxo apresentado, o atendimento se inicia na abertura de um tíquete. Este pode conter uma requisição feita pelo cliente, o qual possui um fluxo próprio e comum de atendimento realizado pela operação e que não é discutido no presente trabalho, por estar fora do tratamento dado a incidentes. Se o mesmo for classificado como um incidente, verifica-se se há algum tipo de anomalia no ambiente, que possa justificar o problema. Caso seja identificada a anomalia, tenta-se isolar e determinar a localização do problema no sistema ou nos equipamentos de rede. Sendo possível o isolamento do problema, são tomadas as ações para solução do problema, e ocorre o reporte ao nível gerencial sobre as ações tomadas, e a documentação das mesmas no tíquete, para encerramento do incidente. Não sendo possível isolar e determinar a localização do problema é realizada uma conferência com os demais times responsáveis pelo suporte a outros equipamentos e sistemas que compõem a solução, como aplicação e sistema operacional, por exemplo, para acompanhamento do problema, tendo como objetivo o diagnóstico do mesmo. Havendo a identificação do problema por meio da conferência, identifica-se se as ações para solução do mesmo dependem da operação de gerenciamento de redes. Caso sejam dependentes da operação, são seguidos os passos já descritos para isolamento e determinação de localização do problema. Caso as ações para a solução do problema não dependam da operação de gerenciamento de redes, é realizada a documentação de tal informação no tíquete, e o mesmo é encerrado. É

previsto um reporte gerencial a cada período de 30 minutos durante a conferência com os demais times de suporte, enquanto o problema não foi identificado.

5.4. A implementação

Para que fosse possível iniciar a validação dos processos, assim como do método MALF proposto no presente trabalho, utilizou-se o processo do MACN, já apresentado na seção 3.2. Para sua utilização, iniciou-se a apresentação de seu funcionamento em uma reunião juntamente com a equipe de negócio da empresa cliente, cujo objetivo foi o entendimento de quais sistemas seriam considerados essenciais ao funcionamento do negócio da companhia.

Mediante esta reunião, verificou-se um ambiente denominado *Desktop* Virtual (DV), cuja funcionalidade é prover ao usuário a sua área de trabalho, localizado em um servidor fisicamente instalado no DC, como um ambiente propício para prática e validação dos processos propostos, dada a criticidade que a indisponibilidade desse ambiente possui, por ser utilizado como ambiente computacional de 90% dos usuários da companhia.

Utilizou-se então do MACN para identificar todos os equipamentos, servidores e sistemas que compõe a solução do DV, a interligação entre os mesmos, a conexão de rede dos servidores, e entre os diversos equipamentos conectados ao sistema de telecomunicações que são utilizados por esse ambiente. Também foi possível identificar os fluxos de comunicação entre os sistemas e seus componentes, possibilitando mapear todos os componentes físicos e lógicos que o sistema se utiliza em seu funcionamento. Este mapeamento possibilitou a visibilidade do que representa o DV, com relação aos servidores e equipamentos de rede que constituem o ambiente. Havia uma especial preocupação do cliente com relação à precisão no diagnóstico de um problema, pois com uma quantidade de usuários internos e externos da empresa, utilizando o ambiente para inserção de dados referentes a vendas, questões logísticas bem como campanhas e marketing, compra de insumos para a fabricação de produtos, dentre outros, a margem de erro tolerável no processo de diagnóstico de um problema ou falha torna-se muito próxima de zero, e com um tempo muito restrito para a localização do problema.

Ao final do mapeamento realizado, tornou-se possível identificar a composição da solução completa, a qual é apresentada a seguir:

- Número de servidores virtuais: 238;

- Número de servidores físicos: 40 *BladeCenters* utilizando-se de *VMWARE* como software de virtualização;
- Número de *switches* de acesso: 12 *switches* para os *BladeCenters* com *uplink* de 10Gbps;
- *Switches* de distribuição: 4 switches de distribuição, compostos com mais de 900 portas de rede;

O mapeamento realizado resultou na construção de uma topologia do ambiente, que é apresentada na Figura 19.

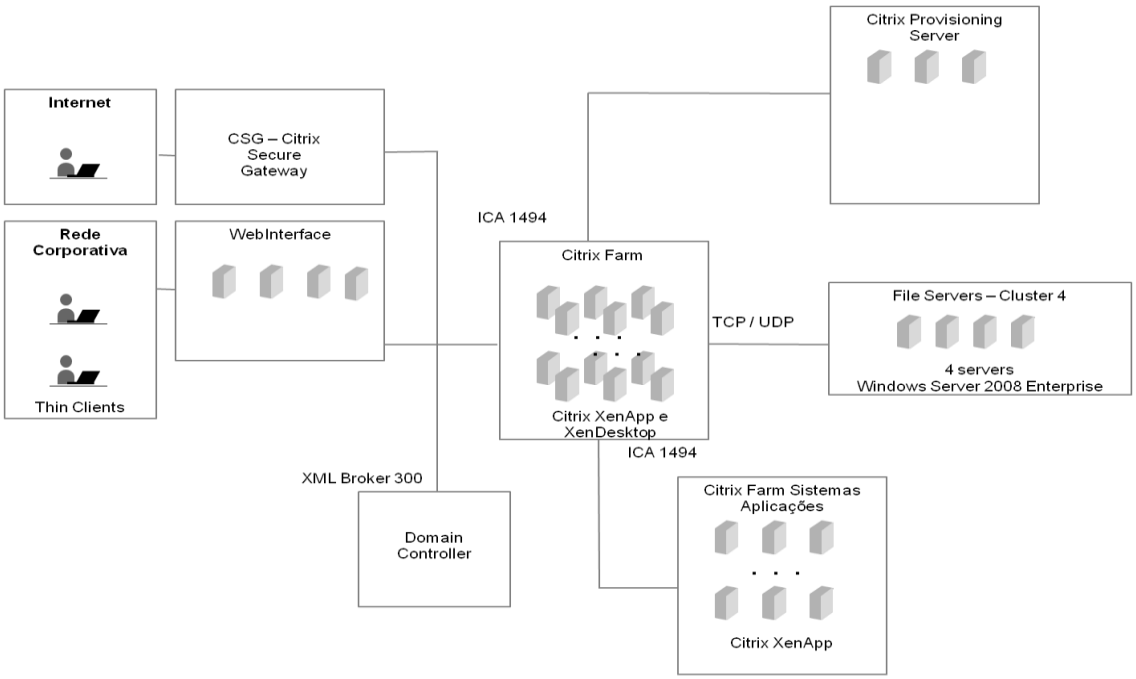

Figura 19 – Estrutura dos servidores localizados no DC.

Aplicando-se o MACN também se efetuou o mapeamento de todas as conexões físicas e lógicas dos *BladeCenters* onde estão os servidores físicos e virtuais do ambiente apresentado. Tal mapeamento é exibido na Figura 20.

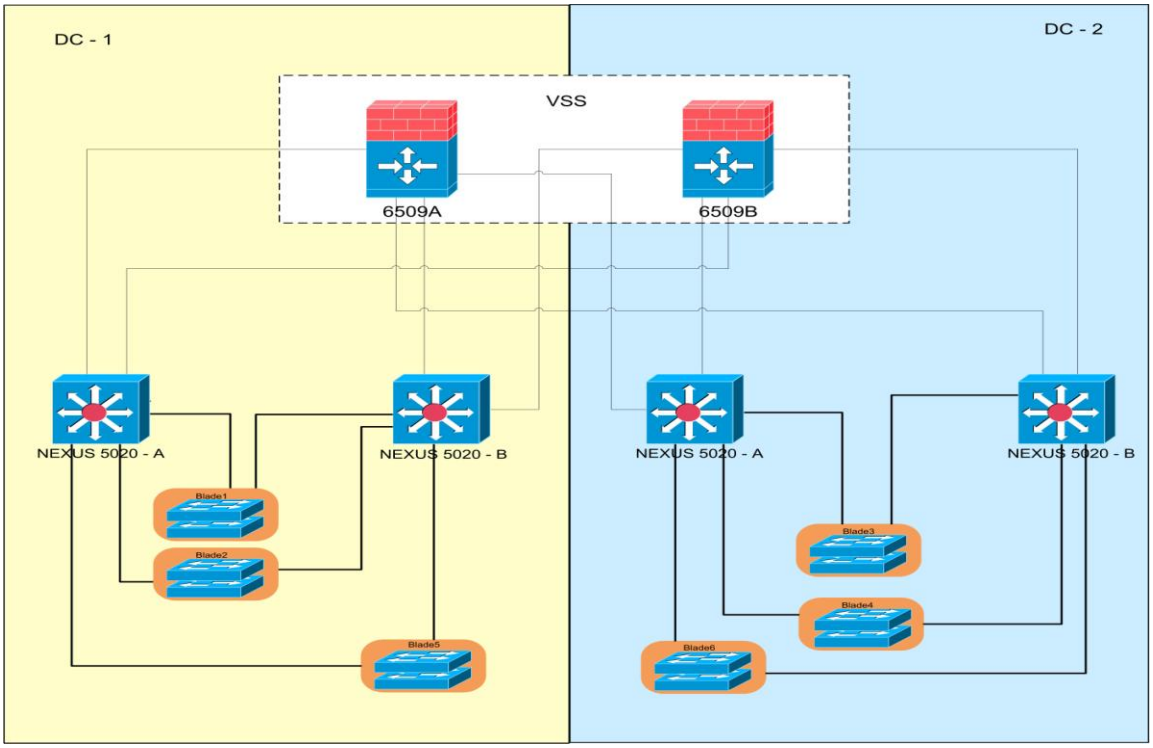

Figura 20 - Topologia da rede onde se encontra o ambiente DV

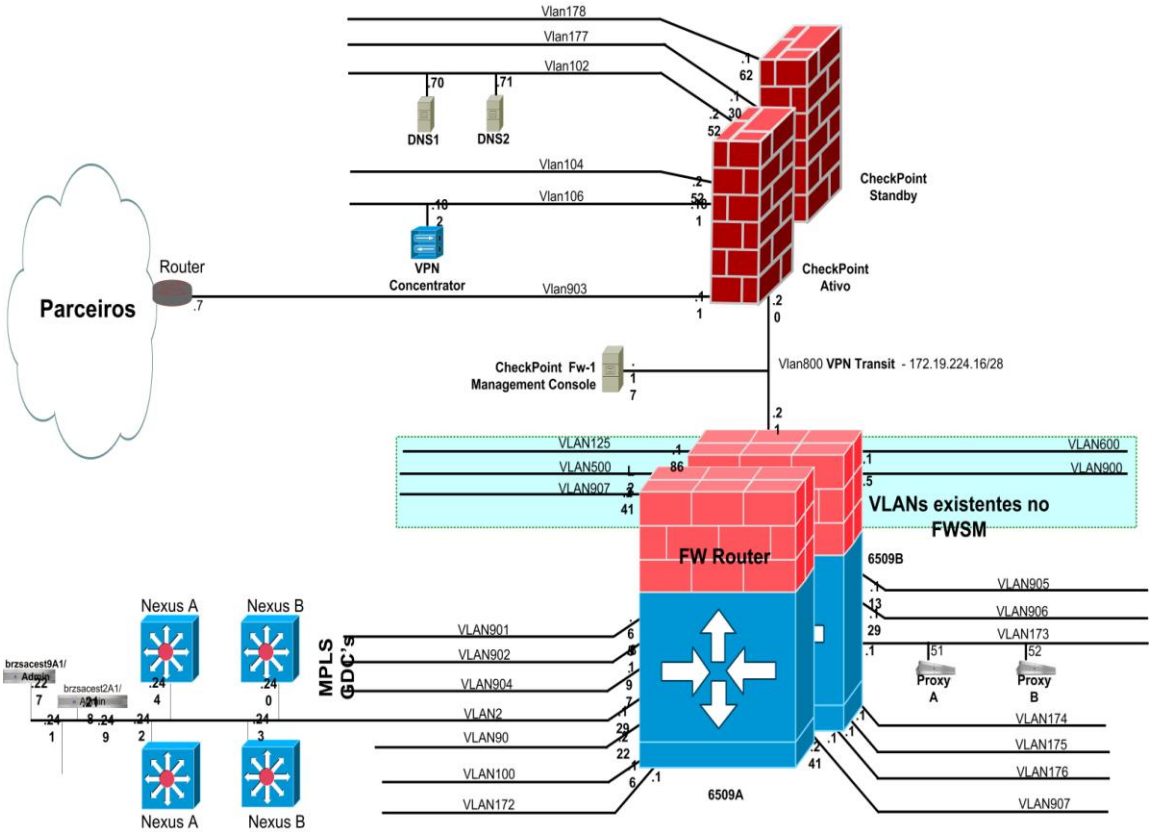

Figura 21 - Topologia lógica da rede - ambiente DV

Na topologia de rede apresentada, demonstra-se o caminho da conectividade física e lógica do ambiente de DV, desde os *switches* internos do *BladeCenter* onde estão os servidores virtuais que compõem o ambiente*, as conexões destes* até os *switches* de distribuição que compõe a estrutura, identificando cada interface entre equipamentos, e permitindo mediante tal levantamento a visibilidade total do cenário que compreende a aplicação selecionada para a validação do método. Na Figura 21 são apresentados os equipamentos que atuam como *gateway,* provendo o controle de fluxo entre os muitos segmentos de rede existentes, assim como mostra em quais segmentos há proteção por camadas de *firewall*, comunicação com a Internet, acesso a rede de parceiros e zonas desmilitarizadas, que são segmentos de rede acessíveis pela internet todavia protegidos por firewall. A construção da topologia e do mapeamento realizado pelo MACN possibilitou a utilização do processo da LVR, o qual no ambiente apresentado irá identificar se existem falhas, anomalias ou mau funcionamento nos equipamentos do sistema de telecomunicações em casos de problemas que não possuem a causa raiz clara, ou ainda não é possível sua identificação. Para que fosse possível a utilização os processos nos eventos posteriores a implementação dos mesmos no ambiente, foram criados procedimentos para o *Help Desk,* de forma que houvesse a classificação de cada tíquete relatando um evento que estivesse relacionado ao ambiente de DV. Solicitou-se a verificação de algumas informações junto ao reclamante, como o número de usuários impactados pelo problema, ou ainda se a indisponibilidade era atribuída a algum sistema específico ou ao ambiente em sua totalidade, para uma melhor qualificação do cenário problemático. Também se estruturou a operação, para que o fluxo proposto na Figura 15 fosse seguido. Estes procedimentos possibilitaram a operação da provedora de serviços de telecomunicações, caso um evento (tíquete) fosse classificado como crítico no atendimento inicial, o acionamento imediato do coordenador e gerente da área de operação e provimento do serviço. Tal acionamento tem como finalidade a interação imediata com o cliente, com o objetivo de validar o impacto bem como atuar junto à operação para identificar e corrigir os problemas, identificando a causa raiz do mesmo. Também é objetivo do acompanhamento executivo intensificar o foco do time na solução do problema, demonstrando ao cliente sinergia e atenção total para o restabelecimento do ambiente, além de cuidado com o negócio do cliente.

A implementação dos processos propostos neste trabalho demandou um período de tempo de aproximadamente quatro semanas, abrangendo a documentação de todo o ambiente de rede, que compreende desde a porta dos servidores onde a aplicação está inserida incluindo todo o caminho através dos sistemas que são utilizados para a comunicação com os demais servidores com os quais o sistema estabelece conexões. O

processo de documentação e procedimentos junto à operação da provedora dos serviços de rede e com o *Help Desk* demandou um tempo de uma semana. Para que o resultado pudesse ser bem avaliado e abrangesse os períodos de sazonalidade e demanda da empresa cliente, optou-se por utilizar o mesmo período de tempo para validação dos resultados.

5.5. Os resultados

Como resultado da implementação descrita na seção anterior, um mapeamento completo da aplicação DV, com seus fluxos de comunicação pôde ser realizado e documentado. Este mapeamento possibilitou identificar falhas existentes no ambiente e que, devido à falta de uma visão completa do sistema e dos fluxos de comunicação, não haviam sido mitigadas e solucionadas. Adicionalmente, o mapeamento do DV possibilitou identificar vulnerabilidades no ambiente, bem como justificar investimentos para a solução destas vulnerabilidades, conseqüentemente aumentando a estabilidade e disponibilidade deste ambiente. Como resultado deste mapeamento, houve um nível de detalhamento bastante elevado dos componentes, bem como do sistema de comunicação do ambiente DV, com suas dependências, possibilitando uma rápida identificação de elementos na solução, visando um diagnóstico preciso em caso de incidentes.

Quanto às falhas, identificou-se que, no ambiente, havia caminhos de comunicação entre *switches* de rede que em alguns momentos apresentavam alta utilização, afetando o desempenho da aplicação. Mediante tal mapeamento, não houve problemas em justificar o investimento para troca de interfaces de rede e aumento da taxa de transmissão das mesmas. Também se identificaram interfaces de rede utilizadas por servidores, configurados com parâmetros e taxa de transmissão diferente da recomendada para o cenário em questão, de acordo com as melhores práticas recomendadas pelos fabricantes e desenvolvedores da solução, sendo que tal ajuste resultou em melhoria de desempenho do tráfego entre os equipamentos. Esse resultado foi possível pela execução da LVR no ambiente apontado pelo MACN, a fim de atestar a condição do ambiente, bem como mitigar falhas antes do primeiro evento após a prática dos processos, sendo este outro diferencial identificado. Mesmo sendo o propósito dos processos o diagnóstico e tratamento de incidentes, possibilitou-se, mediante sua prática, aplicada no momento de implementação dos processos, verificar se a parametrização e funcionamento dos equipamentos que compõem o ambiente do DV estavam em sua melhor configuração e livre de erros operacionais ou de projeto. Cada uma das conexões

mapeadas e documentadas, conforme exibido na Figura 19, Figura 20 e Figura 21, foram atestadas pela LVR, quando aplicável, a fim de validar seu correto funcionamento, bem como sua configuração de acordo com as melhores práticas recomendadas pelos fabricantes para o cenário utilizado, como taxa de transmissão da interface de rede, comunicação entre equipamentos que compõem o sistema de comunicação, dentre outros parâmetros.

Após a utilização da MACN, qualquer incidente relacionado ao ambiente DV, independente da severidade associada ao tíquete, seria priorizado. Essa abordagem oferece uma nova perspectiva de entrega do serviço, que não está baseada em um nível de serviço acordado apenas, mas sim associada à necessidade de negócio do cliente. Como resultado da prática dos processos, ao observar o mesmo período no ano seguinte, foi possível identificar uma incidência menor de eventos no ambiente. Tais dados são mostrados a seguir:

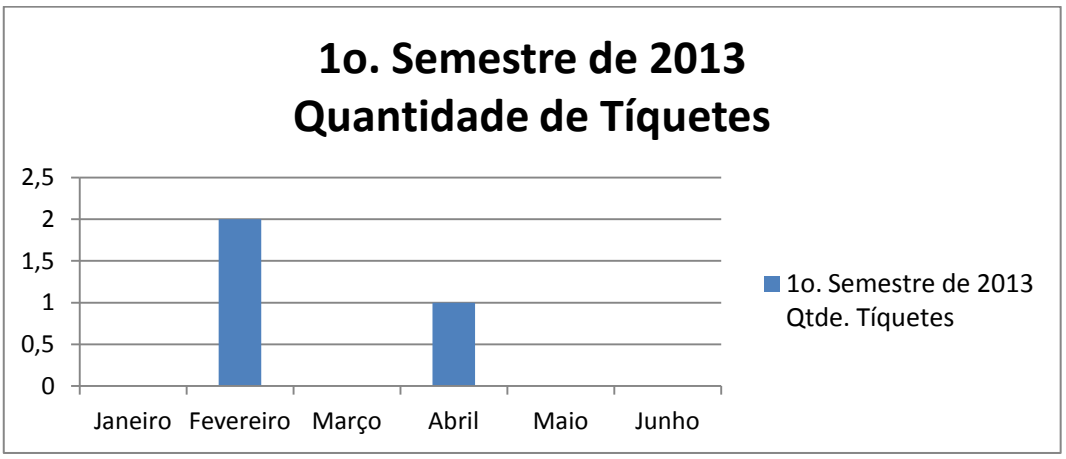

Figura 22 - Volume mensal de tíquetes abertos pelo cliente em 2013

Na Figura 23, são exibidos os dados comparativos, considerando os dois períodos avaliados.

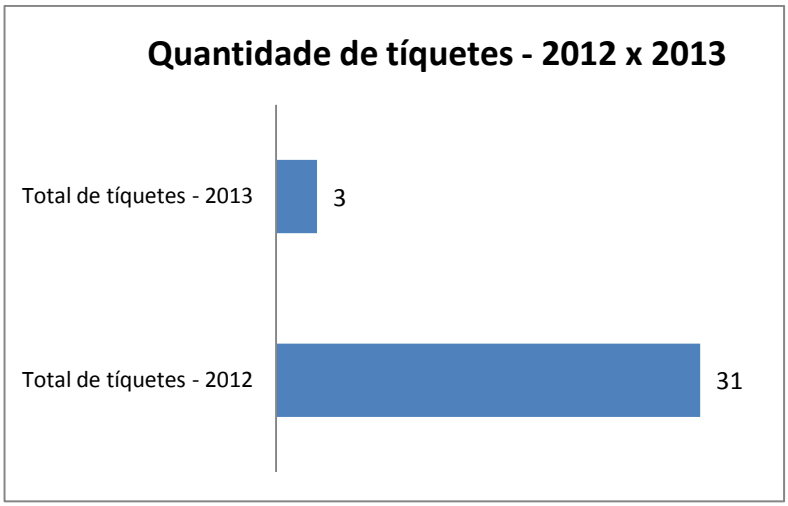

Figura 23 - Comparativos de volumetria de tíquetes abertos pelo cliente em 2012 X 2013

Observou-se, através dos resultados coletados no primeiro semestre de 2013, e confrontados com o mesmo período no ano anterior, uma redução significativa no número de tíquetes abertos pelo cliente para a provedora de serviços. No ano de 2013, este número de tíquetes foi de apenas três, sendo que apenas um foi classificado como severidade 1. Tal redução expressou uma redução de mais de 90% no número de incidentes abertos, comparando-se o mesmo período em anos anteriores, como descrito acima. Dentre as razões para tal redução, está a prática dos processos, os quais foram executados no período de implantação como medida inicial, a fim de garantir que os mesmos refletiam o mapeamento realizado e as necessidades do ambiente, bem como sua correta configuração.

Foi efetuada a comparação deste incidente com outro, ocorrido em 2013, cujos dados são apresentados a seguir:

Evento	Detalhes
1	**Descrição**: SUMÁRIO: **Desktop Virtual - DV** - Lentidão para todas as unidades DETALHES: Lentidão no DV principalmente na unidade XXX. Acesso via WEB também sendo afetado **Data e hora da abertura**: 04/02/2013 10h37min **Data e hora do encerramento**: 04/02/2013 12h28min **Tempo de atendimento**: 01h50min hora **Solução**: SINTOMA: Rede 172.19 apresentando lentidão ao mapear FS através dos servidores dessa rede. CAUSE: Não identificado. SOLUÇÃO: Em conferência com demais times, e contatando o cliente, fomos informados que não há mais problemas de lentidão. Efetuamos análise no ambiente de redes e não foi encontrado problemas. Fluxo analisado: 172.19.249.14 para 172.19.248.35

Tabela 8– Eventos coletados no ano de 2013, relacionados ao ambiente de DV

Neste evento, o cliente informa lentidão em seu ambiente, especificamente no acesso a arquivos localizados em servidores no ambiente. Este incidente foi relatado pelo cliente às 10h37min e foi encerrado às 12h28min. Para o incidente em questão, foi utilizado o fluxo proposto pelo presente trabalho, apresentado na Figura 15, para o diagnóstico e tratamento do incidente. Verificou-se que:

- Na abertura do tíquete, o *Help Desk* classificou o incidente como crítico, por estar relacionado ao ambiente DV;
- Imediatamente o nível gerencial da provedora de serviços iniciou o acompanhamento do incidente, entrando em contato com o cliente para qualificar o nível de impacto, que neste caso refletia apenas a indisponibilidade de acesso a informações de arquivos de usuários do DV;
- Utilizou-se o MACN para identificar quais servidores possuíam a função de servidores de arquivos no ambiente do DV. Essa informação consta no final do atendimento, conforme descrito no evento 2;
- Executou-se a LVR, para garantir que todas as parametrizações de configuração de interfaces dos servidores, bem como a comunicação realizada entre os mesmos estavam livres de erros e com o correto funcionamento, assim como os equipamentos que fornecem a

conectividade do sistema de telecomunicações que atende o ambiente em questão;

- Tão logo foram realizados estes procedimentos, efetuou-se contato com as outras áreas de suporte, em uma conferência realizada com a participação do cliente, a fim de informar todas as ações executadas e identificar juntamente com as demais equipes de suporte a causa do problema;
- Houve clareza para o cliente, após serem fornecidas as informações das verificações efetuadas, que o problema não estava relacionado ao sistema de telecomunicações e, apesar de não ser identificada a causa do problema, o cliente demonstrou satisfação com a operação pelo alinhamento, clareza e acompanhamento gerencial do problema, informando que era a primeira vez que se sentia confortável com o resultado do diagnóstico efetuado pela operação de telecomunicações.

Verificou-se também, o resultado da prática dos processos nos demais tíquetes abertos para o ano de 2013, mesmo não se tratando de incidentes críticos, uma vez que os mesmos eram poucos e para um melhor resultado do método.

Evento	Detalhes
2	**Descrição**: SUMÁRIO: Problema de Comunicação DETALHES: Os IPs e portas alocadas no chamado XXXX, não estão respondendo na mesma rede. Obs. Almir alinhado do problema Qualquer dúvida, favor entrar em contato no fone: Cel. (19) XXXX ou com o XXX@ no fone 19-XXXX **Data e hora da abertura**: 28/02/2013 19h44min **Data e hora do encerramento**: 01/03/2013 13h51min **Tempo de atendimento**: 04h51min **Solução**: SINTOMA: Problema de Comunicação. CAUSA: Falha operacional na configuração dos servidores SOLUÇÃO: Chamado encerrado conforme notas abaixo: From: XXX@XXX Sent: sexta-feira, 1 de março de 2013 13h45min (evidência da autorização para encerramento do chamado)

Tabela 9– Tíquete de severidade 4 – Teste da LVR

O tíquete relatado no evento 3 informava uma falha de funcionamento na configuração de IP e interfaces de rede alocadas para novos servidores na rede. Para

esse incidente, não se utilizou o MACN e o AEIC, pois não se tratava de um incidente crítico. Verificou-se através da utilização da LVR, que a configuração realizada nas interfaces de rede que iriam atender os servidores a serem ativados estava correta, considerando-se que os servidores estavam inseridos em uma mesma rede e de acordo com a solicitação. Para esse caso em específico, por se tratar de um tíquete de severidade 4, aberto fora do horário comercial, que compreende o período entre 09h00min até às 18h00min, foram consideradas somente as horas dentro deste intervalo. O tempo para execução da LVR foi de aproximadamente 30 minutos. Identificou-se através da execução da LVR, que havia informação de endereço *Medium Access Control* (MAC) nas tabelas de endereçamento dos *switches* em que estavam conectados os servidores. Em conferência com a equipe responsável pela ativação dos servidores, identificou-se uma falha operacional na configuração dos mesmos, pois por se tratar de um *BladeCenter*, identificou-se que a interface de rede dos servidores estava invertida com as lâminas inseridas no BladeCenter, ocasionando a falha. Uma vez corrigidas as configurações, o equipamento passou a operar normalmente e o fluxo de comunicação de tais servidores com o restante da rede estava funcionando como esperado.

Quanto ao terceiro tíquete, apresentado abaixo na Tabela 10, não foi possível efetuar qualquer diagnóstico, pelo fato do tíquete ter sido aberto de forma incorreta para a operação da provedora de serviços, pois o serviço reclamado estava fora do escopo de serviço da mesma.

Evento	Detalhes
3	**Descrição**: SUMMARY: Problema de recebimento de email do site XXXX DETAILS: Segue log: Mails which we are not able to deliver due to problems with remote host are retried based on standard retry schedule. Root of the problem here is that remote server is not able to respond in a timely fashion. **Data e hora da abertura**: 25/04/2013 17h46min **Data e hora do encerramento**: 29/04/2013 09h26min **Tempo de atendimento**: 87h39min horas **Solução**: SYMPTON: Problema de recebimento de email do site XXX CAUSE: Necessidade do cliente RESOLUTION: Cliente autorizou fechamento do chamado. Solução do problema fora do escopo.

Tabela 10– Tíquete de severidade 2 - fora de escopo.

A implementação dos processos de MACN e da LVR, possibilitou um efetito preventivo, uma vez que sua utilização possibilitou verificar as falhas antes mesmo da sua utilização para tratamento de incidentes, o que resultou na diminuição no número de

eventos, exibidos na Figura 23. Esta prevenção é uma característica que não foi planejada na concepção dos processos, e que somente pôde ser verificada mediante sua implementação e validação.

Verificou-se que o processo MACN proporcionou uma facilidade na justificativa de investimento para solucionar pontos de vulnerabilidade ou risco no caminho de comunicação de rede, ou ainda na infraestrutura como um todo, uma vez que o processo permite uma visualização completa dos equipamentos que compõem a solução, fornecendo ao time técnico bem como aos gestores do ambiente, subsídio para justificativa de investimento, tendo visibilidade das fragilidades em ambientes críticos.

Outro ponto importante é observar que o tíquete que foi aberto relatando problemas no ambiente foco desta validação foi rotulado com o nome do ambiente pelo *Help Desk*, neste caso, DV, proporcionando a utilização do AEIC para interação executiva junto ao cliente. Tal ação demonstrou-se eficiente na visão do cliente, pois o mesmo não havia presenciado outrora um gerente ou executivo contatando a empresa cliente para informar sobre a ciência do problema por parte dos executivos da prestadora de serviços antes mesmo de qualquer processo de escalonamento. Segundo o cliente, tal ação demonstrou maturidade da empresa no fornecimento do serviço, bem como preocupação com o negócio do cliente, trazendo satisfação do mesmo com os serviços prestados.

Quanto aos demais incidentes, o processo LVR demonstrou-se eficaz para diagnosticar se havia ou não falhas no ambiente de rede, pois rapidamente executaram-se verificações em todo o caminho de rede por onde os servidores do ambiente se comunicavam. Na ausência de falhas, coube à provedora de serviços o acompanhamento do problema junto aos demais times de suporte apenas. O resultado da prática dos métodos foi a inexistência de diagnóstico de falhas nos sistemas de telecomunicações gerenciados pela provedora de serviços nos tíquetes abertos no período do primeiro semestre de 2013. O cliente também demonstrou grande satisfação e tranqüilidade em saber que havia uma lista de itens a serem verificados e validados durante um problema para garantir a inexistência de falhas comuns ou resultantes de uma mudança ou falha operacional. Um ponto a ser destacado sobre tal processo de validação foi que, como as vulnerabilidades foram identificadas e, conseqüentemente, sanadas na etapa de implementação do processo, notou-se uma grande clareza no diagnóstico dos problemas, mesmo antes da utilização da LVR para diagnóstico.

5.6. Aplicação do método em outros cenários

Como resultado dos processos criados, bem como da proposta de fluxo, utilizou-se o provimento dos serviços de gerenciamento de rede da provedora para 68 empresas clientes de diversos tamanhos e objetivos de negócio, para identificar a aplicabilidade da proposta apresentada no presente trabalho no cenário dos demais clientes. Para tal, classificaram-se as empresas analisadas, as quais foram divididas em 3 categorias conforme os aspectos de porte, volume, complexidade e criticidade de cada uma delas:

Categoria 1 - Empresas de grande porte que fatura acima de R$500 milhões anuais, que possuem mais de 10 mil funcionários e operando em diversas localidades;

Categoria 2 - Empresas de porte médio, ou seja, que possua um faturamento de entre R$100 milhões até R$500 milhões anuais, que possuem suas aplicações concentradas em servidores alocados em um CPD e possuem ligação com a Matriz à qual são conectadas as demais filiais, e possuem de 1 mil a 10 mil usuários;

Categoria 3 - Empresas de pequeno porte, ou seja, que possuem faturamento inferiora R$100 milhões anuais, que possuem suas aplicações e servidores alocados no CPD que pode ser local ou remoto e possuem menos de 1 mil usuários;

A Figura 24 apresenta o resultado da classificação das empresas.

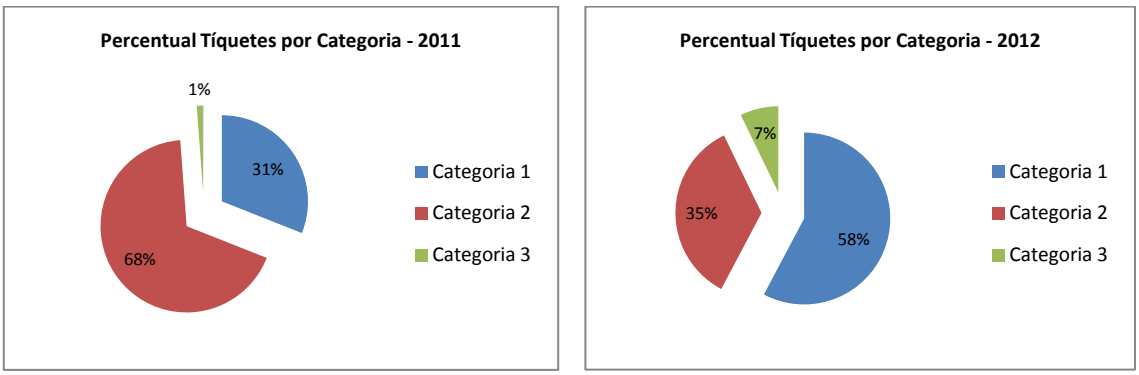

Figura 24 – Volumetria de tíquetes no período de 23 meses.

Conforme a figura apresentada há uma incidência maior de tíquetes abertos por grandes empresas, se comparado a empresas de menor porte. Tal classificação teve por objetivo identificar a demanda de tíquetes por porte de clientes a fim de identificar o impacto de cada categoria na volumetria de incidentes, entendendo-se que clientes de maior porte possuem ambientes mais complexos.

Todos os clientes classificados como Categoria 1, possuem cenários críticos, nos quais o uso do MACN e do AEIC pode ser implementado, com bons resultados, havendo a possibilidade, inclusive, de apresentar uma proposta diferenciada de nível de serviço não associado à classificação de severidade atribuída a um chamado, mas sim, alinhado com as necessidades de negócio de cada um dos clientes, e seus ambientes. Há ainda, a possibilidade de implementação de uma área de relacionamento, a qual tem por objetivo acompanhar os incidentes críticos provenientes dos tíquetes abertos e classificados como tal, para um alinhamento e suporte do nível gerencial e executivo da provedora de serviços na tomada de decisão associada a operação e a estratégia de relacionamento com os clientes.

Prosseguindo com a aplicação, durante o período de 23 meses, observaram-se 8581 tíquetes de problemas, os quais foram utilizados como cenário para complementar a validação da funcionalidade dos processos e da proposta de fluxo descrita no presente trabalho. Efetuou-se a separação dos dados de acordo com os tipos de eventos. A classificação destes dados foi fornecida pela provedora de serviços, e é exibida na Figura 25:

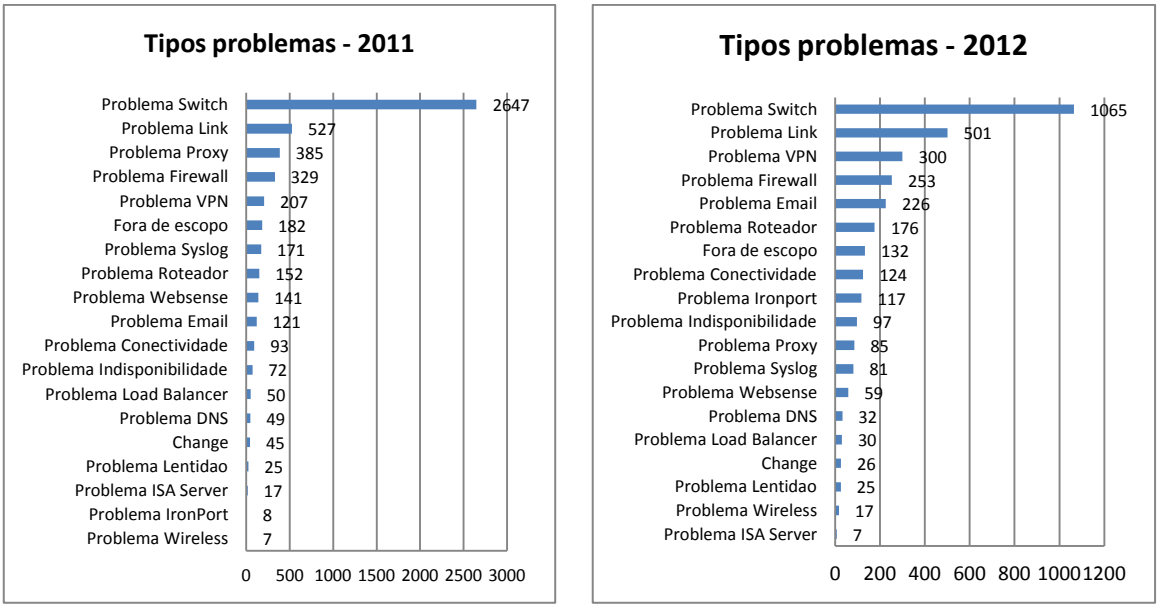

Figura 25 – Classificação dos tipos de problemas identificados e classificados nos anos de 2011 e 2012

Mediante a separação e classificação dos dados, identificou-se que 56% do total de problemas verificados na volumetria, concentram-se em apenas 2 categorias dos problemas analisados. Analisaram-se então as causas primárias dos eventos mais relevantes. A causa primária é a razão pela qual um evento de problema ocorreu, como um erro operacional, uma falha de energia. Tais causas são apresentadas na Figura 26.

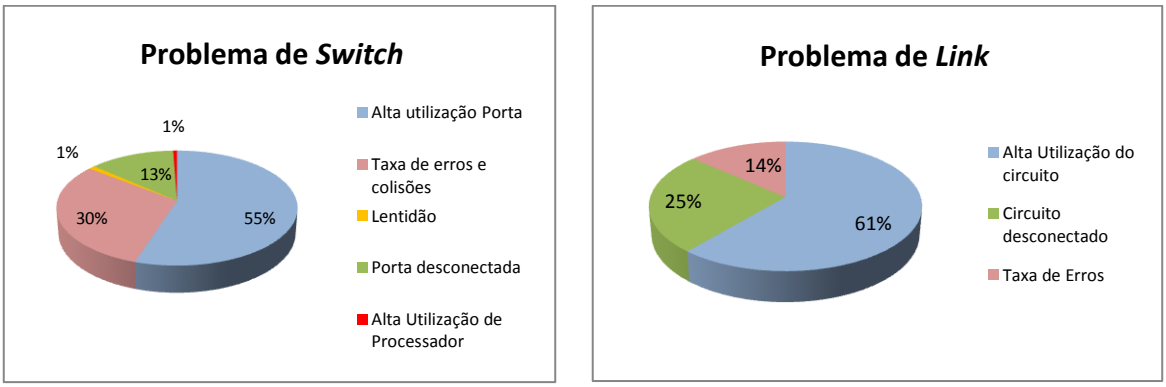

Figura 26 – Volumetria das causas primárias da categoria "Problema de Switch" e "Problemas de Link"

A seguir, é realizado o detalhamento das causas primárias:

Problema de Switch: Entende-se qualquer problema que foi identificado a partir de um tíquete relacionado a algum equipamento conectado a um switch e cujo problema tenha relação direta com o mesmo. A partir dessa classificação identificou-se:

- **Alta Utilização**: Utilizada quando é diagnosticado que uma porta está utilizando uma banda acima do limite aceitável, neste caso estabelecido em 90%.
- **Taxa de Erros**: Classificação atribuída quando são identificados erros ou colisões nos contadores das portas de switch nas quais se encontram conectados equipamentos ou servidores.
- **Lentidão**: Classificação atribuída quando se identifica algum tipo de demora na transmissão de dados entre equipamentos, sendo que pelo menos um dos membros da comunicação está conectado ao switch em questão.
- **Porta Desconectada**: Classificação atribuída a uma porta que teve seu estado alterado de “porta conectada” para “porta desconectada”, indicando desta forma uma desconexão do equipamento outrora conectado à mesma.
- **Alta Utilização do Processador**: Classificação atribuída ao uso do processador em uma taxa acima de 90%. Normalmente nesta classificação, este estado ocasiona impacto no ambiente por tal utilização degradar de forma drástica o desempenho do equipamento.

Problema de Link: Entende-se qualquer problema que foi identificado a partir de um tíquete relacionado à conectividade de um circuito de dados (link) interligando ao menos duas localidades.

- **Alta Utilização**: Utilizada quando é diagnosticado que o link está utilizando uma banda acima do limite aceitável, neste caso estabelecido em 90%.
- **Taxa de Erros**: Classificação atribuída quando são identificados erros ou colisões nos contadores das portas de conexão com o circuito de dados.
- **Porta Desconectada**: Classificação atribuída a uma porta que possui um link a ela conectado e que teve o seu estado alterado de “porta conectada”

para “porta desconectada”, indicando desta forma uma desconexão do equipamento conectado à mesma.

A partir do detalhamento do cenário utilizado é exibida abaixo a aplicação dos processos e do método MALF.

Lista de Verificação de Rede (LVR) – Verificou-se que a LVR aborda todos os pontos identificados nas causas primárias, nas categorias “Problemas de Switch” e “Problemas de Link”. Pode-se afirmar que a utilização da LVR é suficiente para evitar que mais de 50% dos incidentes fossem relatados pelos clientes em um período de 23 meses.

Mapeamento de Ambientes Críticos ao Negócio (MACN) – Para utilização do MACN, seria necessário um processo de mapeamento em conjunto com os 68 clientes da provedora de serviços, identificando em cada cliente quais sistemas são considerados críticos para o funcionamento do negócio dos mesmos. A partir de tal identificação é possível seguir o processo de mapeamento descrito na Figura 8 para correlacionar os sistemas críticos ao negócio ao ambiente de rede, documentando tais sistemas. No fluxo apresentado na figura 5, a MACN, então, permitirá uma visibilidade técnica do sistema de negócio no qual o incidente está contextualizado, possibilitando a rastreabilidade do problema nos diversos componentes e equipamento do ambiente. Aplicado em conjunto com a LVR, proporciona a rastreabilidade de eventos de falha em ambientes críticos.

Acompanhamento Executivo de Incidentes Críticos (AEIC) - No levantamento efetuado identificou-se que em 90% dos casos que ocorreu o processo de escalonamento por parte do cliente para atenção e agilidade na solução do problema, a linha executiva da empresa provedora dos serviços não tinha conhecimento do problema. A abordagem do AEIC possibilita um conhecimento do problema por parte do nível executivo e ações estratégicas antes que o processo de escalonamento ocorra. Sua utilização no cenário deve ocorrer sempre que um incidente for categorizado como crítico pela MACN.

Identificou-se que a operação da provedora de serviços possui um fluxo de atendimento de incidentes que não prevê o mapeamento dos incidentes críticos como fator de decisão para priorização no atendimento pela operação da provedora de serviços. Não existe comunicação com o nível executivo no momento de identificação do

incidente crítico, dado que a única forma existente para determinação da criticidade é o nível de severidade que um tíquete é classificado, ou a escalada de um problema ao nível executivo. Adicionalmente, não se identificaram na estrutura da operação antes da implementação do método MALF, um procedimento de verificação de elementos de rede, e o gerenciamento de incidentes, em tempo real com o intuito de diagnosticar se o mesmo está relacionado com itens físicos ou lógicos. O método MALF proposto, apresenta processos que complementam o fluxo descrito no modelo Z, uma vez que tais processos permitem um melhor gerenciamento do tratamento de incidentes, utilizando a base de conhecimentos como aperfeiçoamento para o diagnóstico dos eventos, gerenciamento da crise mediante o acompanhamento executivo e técnicas para o diagnóstico do problema.

6. Conclusão

Identificaram-se benefícios na prática da proposta descrita no presente trabalho, pois esta aplicada aos ambientes no processo de validação proporcionou de fato, conforme resultado da prática dos processos em um cliente, aperfeiçoamento e rastreamento no diagnóstico e tratamento dos eventos relatados, com especial atenção à resolução definitiva de problemas. Há uma interação com o nível executivo da provedora de serviços para acompanhamento e verificação dos possíveis impactos para o negócio do cliente, o que resultou em uma satisfação do cliente e em novos negócios para a provedora de serviços, em serviços antes oferecidos por outros provedores. A utilização do AEIC, para o acompanhamento executivo de tais eventos a partir do momento em que um tíquete classificado como crítico chega à operação possibilita mensurar o impacto financeiro e de imagem da empresa cliente em decorrência da falha, suportando a tomada de decisão da gestão da provedora de serviços e do próprio cliente.

Na validação da proposta apresentada, pôde-se atestar a eficácia da LVR, como ferramenta de diagnóstico de falhas ou anomalias na rede. Verificou-se que sua prática em ambientes críticos previamente mapeados pode oferecer precisão e rapidez no diagnóstico de falhas e problemas, diminuindo o tempo de indisponibilidade e impacto para o negócio dos clientes. Entende-se que um método bem definido e amadurecido de diagnóstico e tratamento de problemas no ambiente de rede possibilitará um modelo preventivo de detecção dos problemas a partir do comportamento de uma anomalia. Um problema diagnosticado e tratado, com sua causa raiz identificada, permite que seja realizada uma documentação do mesmo em uma base de conhecimento para utilização futura caso o evento ocorra novamente. Adicionalmente, há a possibilidade de mapeamento dos indícios e do comportamento do problema, os quais podem fornecer insumos para uma monitoração preventiva, realizada por ferramentas de monitoramento e gerenciamento da rede e dos sistemas de telecomunicações. O MACN possibilitou uma nova perspectiva para identificação de impactos nos ambientes, classificando-os como críticos para o negócio, com base em um alinhamento com foco no que é sensível e essencial para a oferta de produtos e serviços oferecidos aos clientes. Adicionalmente, o MACN oferece a possibilidade de uma nova proposta para o acordo de nível de serviço, baseado na real necessidade e criticidade de negócio, e não mais em severidades e tempos para atendimento.

O fluxo proposto para gerenciamento de incidentes, acrescido dos processos descritos no presente trabalho, oferece uma efetiva melhoria no processo de tratamento dos incidentes em uma operação de sistemas de telecomunicações, em uma abrangência completa, compreendendo desde a abertura de um incidente, seu tratamento até o encerramento.

6.1. Trabalhos futuros

Próximos trabalhos terão por objetivo a automatização dos processos de identificação de cenários críticos, a utilização de métodos para quantificar a experiência do usuário frente a problemas, bem como a implementação da inteligência da LVR em sistemas de monitoração. Pretende-se, adicionalmente, efetuar a validação e verificação de aplicabilidade dos processos propostos em ambientes diversificados, não relacionados à infraestrutura de TI. Deverão ser mensurados os tempos e resultados da implementação da presente proposta, confrontado-os com os tempos e resultados antes da aplicação do método e dos processos. Também como os deverão ser avaliados os benefícios da prática do método nos diferentes tipos de ambiente.

7. Referências Bibliográficas

[1] A. Z. A. Zhuang, X. Q. X. Qiu, H. C. H. Cheng, X. C. X. Chen, and Z. G. Z. Gao, “A management process defining approach for converged services based on eTOM and ITIL,” *Broadband Netw. Multimed. Technol. ICBNMT 2010 3rd IEEE Int. Conf.*, pp. 180–185, 2010.

[2] B. Krogfoss, G. Hanson, and R. J. Vale, “Impact of Consumer Traffic Growth on Mobile and Fixed Networks: Business Model and Network Quality Impact,” *Bell Labs Tech. J.*, vol. 16, pp. 105–120, 2011.

[3] J. P. G. Sterbenz, D. Hutchison, E. K. Çetinkaya, A. Jabbar, J. P. Rohrer, M. Schöller, and P. Smith, “Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines,” *Comput. Networks*, vol. 54, pp. 1245–1265, 2010.

[4] L. Zhu, M. Song, and J. Song, “ITIL-based IT Service Management Applied in Telecom Business Operation and Maintenance System,” vol. 7, no. 2007, pp. 243–246, 2009.

[5] X. Wu, D. Turner, C. Chen, and D. Maltz, “NetPilot: automating datacenter network failure mitigation,” *ACM SIGCOMM …*, 2012.

[6] S. Nikou, H. Bouwman, and M. de Reuver, “The potential of converged mobile telecommunication services: a conjoint analysis,” *info*, vol. 14, no. 5, pp. 21–35, Jun. 2012.

[7] S. Dhar and U. Varshney, “Challenges and business models for mobile location-based services and advertising,” *Commun. ACM*, vol. 54, no. 5, p. 121, May 2011.

[8] S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang, and A. Ghalsasi, “Cloud computing — The business perspective,” *Decis. Support Syst.*, vol. 51, no. 1, pp. 176–189, Apr. 2011.

[9] J. Heidemann, M. Stojanovic, and M. Zorzi, “Underwater sensor networks: applications, advances and challenges.,” *Philos. Trans. A. Math. Phys. Eng. Sci.*, vol. 370, no. 1958, pp. 158–75, Jan. 2012.

[10] V. C. Gungor, B. Lu, and G. P. Hancke, “Opportunities and Challenges of Wireless Sensor Networks in Smart Grid,” *IEEE Trans. Ind. Electron.*, vol. 57, no. 10, pp. 3557–3564, Oct. 2010.

[11] L. Atzori, A. Iera, and G. Morabito, “The Internet of Things: A survey,” *Comput. Networks*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010.

[12] C. Yin, B. David, and R. Chalon, “Use your mobile computing devices to learn - Contextual mobile learning system design and case studies,” *2009 2nd IEEE Int. Conf. Comput. Sci. Inf. Technol.*, pp. 440–444, 2009.

[13] V. Mann, “Correlating user activity with system data for fast detection and diagnosis of system outages,” no. August, pp. 1–12, 2011.

[14] S. Orlowski and R. Wessäly, “SNDlib 1 . 0 — Survivable Network Design Library,” 2010.

[15] J. K. Kim, R. Sharman, H. R. Rao, and S. Upadhyaya, “Efficiency of critical incident management systems: Instrument development and validation,” *Decis. Support Syst.*, vol. 44, no. 1, pp. 235–250, Nov. 2007.

[16] R. Gupta, K. H. Prasad, and M. Mohania, “Automating ITSM Incident Management Process,” in *2008 International Conference on Autonomic Computing*, 2008, pp. 141–150.

[17] L. K. Comfort, “Crisis Management in Hindsight: Cognition, Communication, Coordination, and Control,” *Public Adm. Rev.*, vol. 67, pp. 189–197, Dec. 2007.

[18] R. Ribeiro, M. M. Garcia, and A. L. Las Casas, “Estratégia e vantagem competitiva no mercado brasileiro de telecomunicações: Um estudo de casos múltiplos para o período de 1999 a 2007,” *Rev. Gestão*, vol. 17, no. 3, pp. 297–312, 2010.

[19] M. Roughan, “Robust Network Planning,” pp. 1–41, 2010.

[20] D. A. Patterson, “A Simple Way to Estimate the Cost of Downtime.” pp. 185–188, 2002.

[21] M.-C. Valiente, E. Garcia-Barriocanal, and M.-A. Sicilia, “Applying an ontology approach to IT service management for business-IT integration,” *Knowledge-Based Syst.*, vol. 28, pp. 76–87, Apr. 2012.

[22] G. Baiôco, A. C. M. Costa, C. Z. Calvi, and A. S. Garcia, “IT service management and governance : Modeling an ITSM configuration process: A foundational ontology approach,” in *2009 IFIP/IEEE International Symposium on Integrated Network Management-Workshops, IM 2009*, 2009, pp. 24–33.

[23] (ww.tmforum.org) TeleManagement Forum, “GB921V Release 5.0 Version 1.4.” p. 68, 2005.

[24] H. Susanto, M. N. Almunawar, and Y. C. Tuan, “Information Security Management System Standards : A Comparative Study of the Big Five,” no. October, 2011.

[25] M. Benhima, J. P. Reilly, Z. Naamane, M. Kharbat, M. I. Kabbaj, and O. Esqalli, “Design and implementation of a Telco Business Intelligence Solution using eTOM , SID and Business Metrics : focus on Data Mart and Application on Order-To-Payment end to end process,” vol. 10, no. 3, pp. 331–355, 2013.

[26] G. Lunardi, “Um estudo empírico e analítico do impacto da governança de TI no desempenho organizacional,” pp. 612–624, 2008.

[27] S. Subashini and V. Kavitha, “A survey on security issues in service delivery models of cloud computing,” *J. Netw. Comput. Appl.*, vol. 34, no. 1, pp. 1–11, Jan. 2011.

[28] P. E. Heegaard and K. S. Trivedi, “Network survivability modeling,” *Comput. Networks*, vol. 53, no. 8, pp. 1215–1234, Jun. 2009.

[29] V. Arraj, “ITIL®: the basics,” *Buckinghampshire, UK*, no. July, 2010.

[30] L. C. Rodrigues, E. A. Maccari, and S. A. Simões, “O desenho da gestão da tecnologia da informação nas 100 maiores empresas na visão dos executivos de TI,” *JISTEM J. Inf. Syst. Technol. Manag.*, vol. 6, no. 3, pp. 483–506, Dec. 2009.

[31] L. D. C. Loureiro, “Relacionamento das melhores práticas do Cobit e ITIL para a Governança de TI,” *wwww.aedb.br*, 2012.

[32] A. Cartlidge, A. Hanna, and C. Rudd, *An introductory overview of ITIL V3*. 2007, p. 58.

[33] (ww.tmforum.org) TeleManagement Forum, “Introduction to eTOM,” *Evaluation*, no. C, p. 68, 2005.

[34] F. T. Information and C. S. Industry, “Enhanced Telecom Operations Map ® The Business Process Framework For The Information and Communications Services Industry An Interim View of an Interpreter ’ s Guide for eTOM and ITIL,” no. April, pp. 1–68, 2005.

[35] TMForum - www.tmforum.org, “TM Forum Frameworx 12.5.”

[36] B. Raouyane, M. Bellafkih, M. Errais, and M. Ramdani, “IMS management based eTOM framework for multimedia service,” in *2010 14th International Telecommunications Network Strategy and Planning Symposium (NETWORKS)*, 2010, pp. 1–6.

[37] Y. Tang, “Use of a layered model for air force enterprise management,” in *MILCOM 2000 Proceedings. 21st Century Military Communications. Architectures and Technologies for Information Superiority (Cat. No.00CH37155)*, 2000, vol. 1, pp. 455–459.

[38] I. Akyildiz and X. Wang, “Cross- Layer Design,” *Wirel. Mesh Networks*, no. December, pp. 112–119, 2009.

[39] C. Manso, D. M. Vianna, C. R. Pierantoni, and T. C. França, “Modelos econométricos de estimativa da força de trabalho: uma revisão integrativa da literatura,” 2013.

[40] H. Polidoro and D. Wolf, “Planejamento de trajetória em ambientes com prioridades dinâmicas,” 2010.

[41] N. Tolia, D. G. Andersen, and M. Satyanarayanan, “Quantifying interactive user experience on thin clients,” *Computer (Long. Beach. Calif).*, vol. 39, 2006.

[42] K.-J. T. K.-J. Tan, J.-W. G. J.-W. Gong, B.-T. W. B.-T. Wu, D.-C. C. D.-C. Chang, H.-Y. L. H.-Y. Li, Y.-M. H. Y.-M. Hsiao, Y.-C. C. Y.-C. Chen, S.-W. L. S.-W. Lo, Y.-S. C. Y.-S. Chu, and J.-I. G. J.-I. Guo, “A remote thin client system for real time multimedia streaming over VNC,” *Multimed. Expo (ICME), 2010 IEEE Int. Conf.*, 2010.