

**UNIVERSIDADE DE CAXIAS DO SUL  
CENTRO DE COMPUTAÇÃO E TECNOLOGIA DA INFORMAÇÃO  
BACHARELADO EM SISTEMAS DE INFORMAÇÃO**

**LEONARDO PAIM MAGALHÃES**

**DESENVOLVIMENTO DE UM PROCESSO DE GERAÇÃO  
DE EVIDÊNCIAS PARA ACOMPANHAMENTO DE MUDANÇAS NA RGE**

**CAXIAS DO SUL  
2015**

**LEONARDO PAIM MAGALHÃES**

**DESENVOLVIMENTO DE UM PROCESSO DE GERAÇÃO  
DE EVIDÊNCIAS PARA ACOMPANHAMENTO DE MUDANÇAS NA RGE**

Trabalho de Conclusão de Curso para  
obtenção do Grau de Bacharel em Sistemas de  
Informação da Universidade de Caxias do Sul.

Orientadora Prof<sup>a</sup>. Eliane Gobetti de Camargo

**CAXIAS DO SUL  
2015**

Dedico este trabalho a todas as pessoas que me acompanharam durante o decorrer da minha graduação, mas em especial à minha família, que sempre acreditou em mim, até mesmo quando nem eu acreditei.

## **AGRADECIMENTOS**

Nesta página deixo meus agradecimentos especiais às pessoas que, de alguma forma, me acompanharam e auxiliaram neste trabalho de conclusão.

Primeiramente, agradeço a Deus, pois sem ele, eu não teria conseguido.

Agradeço a minha família pelo apoio constante e insistente que me foi dado em todos os momentos. Do início ao fim deste grande projeto, sua presença e preocupação foram fundamentais.

À minha orientadora, Professora Eliane Gobetti de Camargo, que transformou meu trabalho em um quebra cabeças e conseguiu montar ele de forma a fazer sentido.

A todos os meus amigos, que são tão especiais pra mim, pois não sei como teria sido conquistar a graduação sem sua constante companhia, que me fez tão feliz durante essa longa jornada.

Aos colegas do Grupo CPFL, especialmente da RGE, que tanto me ensinaram nestes anos de trabalho, agregando conhecimento e me ensinando a trabalhar em equipe.

Meus agradecimentos também ao corpo docente e discente que me acompanhou por todos estes anos, e com quem tanto aprendi. Todo conhecimento adquirido durante esse curso me auxiliou para chegar onde estou.

A todos, meu muito obrigado pelo incentivo e pelas palavras de motivação.

*“A menos que modifiquemos a  
nossa maneira de pensar,  
não seremos capazes de resolver  
os problemas causados pela  
forma como nos acostumamos  
a ver o mundo.”*

**Albert Einstein**

## **RESUMO**

O presente trabalho de conclusão de curso tem como objetivo apresentar a elaboração de um processo de geração de evidências referentes ao procedimento de requisição de mudanças para o ambiente de produção do sistema comercial CCS, a ser implantado na empresa RGE. Este processo deve atender requisitos legais propostos na Lei Sarbanes Oxley, conforme solicita a Governança de Tecnologia da Informação do Grupo CPFL à equipe de manutenção dos sistemas comerciais da RGE, aplicando conceitos legais e das boas práticas de auditoria. Para a elaboração do processo serão avaliadas as técnicas, normas e métodos a serem utilizados pelas equipes envolvidas no processo de auditoria. O processo deve suprir uma necessidade do Departamento de Tecnologia de Informação da empresa, com o intuito de atender os controles internos presentes na metodologia de manutenção de sistemas utilizada, abrangendo todas as evidências necessárias para eventuais auditorias de sistemas de informação.

**Palavras-chaves:** Geração de Evidências. Acompanhamento de Mudanças. Auditoria. Processo. Sistemas de Informação.

## **ABSTRACT**

This paper intends to introduce the building of an evidence generation process about the change request procedures to the production environment of commercial system (CCS), being implemented at RGE company. This process must meet legal requirements proposed by Sarbanes Oxley law, as requested by the Governance team of CPFL Group to the commercial systems maintenance team of RGE, through the application of the legal concepts and good audit practice. The techniques are going to be evaluated, as well as the methods used by the people involved in the audit process in order to build this specific process. It may meet IT Departament's needs towards fulfilling the controls included in the maintenance methodology adopted, covering all evidences needed to possible information systems audits.

**Keywords:** Generation of Evidences. Accompaniment of Changes. Audit. Process. Information Systems.

## **LISTA DE FIGURAS**

Figura 1 - Análise e gerenciamento de risco.....	22
Figura 2 - Processo de gestão de riscos .....	23
Figura 3 - Atividade de tratamento do risco .....	25
Figura 4 - Fluxograma proposto para uma mudança.....	39
Figura 5 - Gerenciamento de Mudanças.....	41
Figura 6 - Exemplo de uma requisição utilizada no CCS.....	49
Figura 7 - Processo da RDM em BPMN .....	51
Figura 8 - Janela Pesquisar Registro .....	52
Figura 9 - Início do preenchimento dos dados na criação .....	53
Figura 10 - Informações básicas da RDM .....	54
Figura 11 - Informações para priorização na RDM.....	56
Figura 12 - Informações cronológicas e de configuração na RDM.....	57
Figura 13 - Informações para implementação da RDM .....	58
Figura 14 - Procedimento automático do CRM ao criar a RDM.....	59
Figura 15 - Tarefa de Aprovação da RDM .....	60
Figura 16 - Informações sobre a implementação da RDM e Anotações .....	61
Figura 17 - Execução da RDM .....	62
Figura 18 - Processo de cancelamento da RDM .....	64
Figura 19 - Exemplo de Histórico de Auditoria .....	71
Figura 20 - Premissa para criação da RDM.....	73
Figura 21 - Plano de Testes nas Anotações da RDM.....	73
Figura 22 - Criação e Aprovação da RDM .....	75
Figura 23 - Conclusão da RDM.....	76
Figura 24 - Detalhes dos relatórios SOX.....	78
Figura 25 - Controle de RDMs .....	79
Figura 26 - Fluxo do Cenário de Testes 1 .....	84
Figura 27 - Fluxo do Cenário de Testes 2.....	86
Figura 28 - Fluxo do Cenário de Testes 3.....	88
Figura 29 - Fluxo do Cenário de Testes 4.....	90

## **LISTA DE TABELAS**

Tabela 1 - Implicações da Lei para TI .....	34
Tabela 2 - Controles identificados .....	64
Tabela 3 - Pontos positivos do processo atual .....	65
Tabela 4 - Problemas no processo atual.....	67
Tabela 5 - Passos do Cenário de Testes 1 .....	84
Tabela 6 - Passos do Cenário de Testes 2 .....	86
Tabela 7 - Passos do Cenário de Testes 3 .....	88
Tabela 8 - Passos do Cenário de Testes 4 .....	90

## **LISTA DE ABREVIATURAS E SIGLAS**

ABAP	<i>Advanced Business Application Programming</i>
ABNT	Associação Brasileira de Normas Técnicas
BPMN	<i>Business Process Modeling Notation</i>
CCS	<i>Customer Care and Services</i>
CMMI	<i>Capability Maturity Model – Integration</i>
COBIT	<i>Control Objectives for Information and related Technology</i>
CPFL	Companhia Paulista de Força e Luz
CRM	<i>Customer Relationship Management</i>
GED	Gerenciamento Eletrônico de Documentos
IPO	<i>Initial Public Offering</i>
ISACA	<i>Information System Audit and Control Association</i>
ITIL	<i>Information Technology Infrastructure Library</i>
MDPS	Metodologia de Desenvolvimento de Projetos de Sistemas
MMS	Metodologia de Manutenção de Sistemas
MMSS	Metodologia de Manutenção de Sistemas de Sustentação
RDM	Requisição de Mudança
RGE	Rio Grande Energia S.A.
SAP	<i>Systeme, Anwendung und Programme</i>
SI	Sistemas de Informação
SOX	Lei Sarbanes-Oxley
TI	Tecnologia da Informação

## SUMÁRIO

<b>1</b>	<b>INTRODUÇÃO.....</b>	<b>13</b>
1.1	PROBLEMA DE PESQUISA .....	15
1.2	OBJETIVOS .....	15
1.3	CONTRIBUIÇÃO CIENTÍFICA.....	16
1.4	ESTRUTURA DO TRABALHO .....	16
<b>2</b>	<b>AUDITORIA .....</b>	<b>18</b>
2.1	CONCEITUAÇÃO DE AUDITORIA .....	18
2.2	ANÁLISE DE RISCOS NO PROCESSO DE AUDITORIA .....	21
2.3	CONTROLES DE AUDITORIA .....	27
2.4	TÉCNICAS DE COLETA DE EVIDÊNCIAS .....	29
2.5	CONTROLE DE ACESSOS .....	32
2.6	LEI SARBANES-OXLEY .....	33
2.7	CONSIDERAÇÕES FINAIS .....	35
<b>3</b>	<b>MUDANÇAS EM SISTEMAS DE INFORMAÇÃO .....</b>	<b>37</b>
3.1	IMPLANTAÇÃO DE MUDANÇAS EM SI .....	37
3.2	PONTOS DE CONTROLE EM MUDANÇAS DE SI .....	40
3.3	AUDITORIA DE MUDANÇAS EM SI .....	41
3.4	CONSIDERAÇÕES FINAIS .....	42
<b>4</b>	<b>PROCESSO ATUAL NA CPFL.....</b>	<b>44</b>
4.1	SISTEMA COMERCIAL DA RGE.....	45
4.2	METODOLOGIA MMS .....	46
4.3	REQUISIÇÃO DE MUDANÇA .....	48
4.3.1	<b>Criação da RDM .....</b>	<b>52</b>
4.3.2	<b>Aprovação da RDM .....</b>	<b>59</b>
4.3.3	<b>Execução da RDM .....</b>	<b>60</b>
4.3.4	<b>Cancelamento da RDM .....</b>	<b>63</b>
4.4	ANÁLISE SUMARIZADA DO PROCESSO ATUAL.....	64

4.5	PROBLEMAS DO PROCESSO ATUAL.....	66
4.6	CONSIDERAÇÕES FINAIS .....	68
<b>5</b>	<b>PROPOSTA DE SOLUÇÃO.....</b>	<b>69</b>
5.1	NOVO PROCESSO.....	69
5.1.1	Histórico de Auditoria.....	70
5.1.2	Premissas para criação da RDM .....	72
5.1.3	Criação/Aprovação da RDM .....	74
5.1.4	Conclusão da RDM.....	75
5.1.5	Controle de RDMS .....	77
5.2	DIFERENÇAS ENTRE OS PROCESSOS .....	79
5.3	ORIENTAÇÃO AOS USUÁRIOS .....	81
5.4	CONSIDERAÇÕES FINAIS .....	81
<b>6</b>	<b>TESTE E VALIDAÇÃO DO PROCESSO .....</b>	<b>83</b>
6.1	CENÁRIO DE TESTES 1 .....	83
6.2	CENÁRIO DE TESTES 2 .....	85
6.3	CENÁRIO DE TESTES 3 .....	87
6.4	CENÁRIO DE TESTES 4 .....	89
6.5	AVALIAÇÃO DOS RESULTADOS OBTIDOS .....	91
6.6	CONSIDERAÇÕES FINAIS .....	92
<b>7</b>	<b>CONCLUSÃO.....</b>	<b>93</b>
7.1	TRABALHOS FUTUROS .....	94
<b>REFERÊNCIAS .....</b>		<b>95</b>
<b>ANEXO A – RELATÓRIO DE RDMS ATENDIDAS.....</b>		<b>97</b>
<b>ANEXO B – RELATÓRIO DE RDMS CANCELADAS.....</b>		<b>98</b>
<b>ANEXO C – RELATÓRIO DE RDMS GERAL .....</b>		<b>99</b>
<b>ANEXO D – RELATÓRIO DE RDMS NÃO ATENDIDAS .....</b>		<b>100</b>

<b>ANEXO E – RELATÓRIO DE RDMS REPROVADAS .....</b>	<b>101</b>
<b>ANEXO F – RELATÓRIO AUDITORIA SOX – IMPLEMENTADORES CCS.....</b>	<b>102</b>
<b>ANEXO G – RELATÓRIO DE RDM INDIVIDUAL.....</b>	<b>103</b>
<b>ANEXO H – TEMPLATE DO PLANO DE TESTES DO GRUPO CPFL .....</b>	<b>104</b>
<b>APÊNDICE A – CENÁRIOS DE TESTES REALIZADOS.....</b>	<b>106</b>

## 1 INTRODUÇÃO

A empresa Rio Grande Energia S.A. (RGE), é uma concessionária de distribuição de energia elétrica, responsável pelo fornecimento de energia elétrica no norte e nordeste do estado do Rio Grande do Sul, abrangendo 262 municípios em sua área de cobertura (RGE, 2013).

A área de Tecnologia da Informação (TI) da RGE é responsável por disponibilizar soluções de sistemas e tecnologia. Na TI, a Divisão de Sistemas é responsável por manter os Sistemas de Informação (SI) utilizados na empresa.

O Open-SGC, sistema comercial da empresa, tem a sua manutenção realizada pela equipe de Sistemas Comerciais. Esta equipe, para atender as solicitações dos usuários, segue parcialmente uma metodologia já obsoleta, chamada Metodologia de Manutenção de Sistemas de Sustentação (MMSS).

A MMSS é utilizada parcialmente pois foi baseada em um ambiente bastante diferente da TI da RGE. Logo, não há garantia da precisão das evidências solicitadas em auditorias realizadas na empresa. Estas evidências são imagens, documentos ou depoimentos que são coletados e analisados no momento de auditoria.

A metodologia foi criada na Companhia Paulista de Força e Luz (CPFL), acionista majoritária da RGE. Nas demais distribuidoras do grupo CPFL, o sistema comercial utilizado é diferente do Open-SGC, com outra linguagem de programação e infraestrutura de TI.

Após alguns anos de utilização, a MMSS foi descontinuada e uma nova metodologia de trabalho foi elaborada. Esta nova metodologia, a MMS, se aplica aos sistemas comerciais utilizados nas empresas do grupo, incluindo práticas, recomendações e controles para tratar as solicitações dos usuários.

Em 2004, a CPFL Energia realizou seu *Initial Public Offering* (IPO), listando suas ações no Novo Mercado da BMF&Bovespa e ADRs Nível III da Bolsa de Nova York. Devido a isso, há auditorias que são realizadas para a garantia de qualidade dos sistemas comerciais utilizados na empresa.

Para as auditorias nos sistemas comerciais, o grupo CPFL implementou práticas de governança corporativa adequadas à Lei Sarbanes-Oxley (SOX). A SOX é uma lei norte-americana que exige, por exemplo, que o Presidente e o Diretor Financeiro reembolsem a companhia com seus bônus ou outros benefícios de renda variável caso a empresa anuncie erros em sua contabilidade (PETERS, 2007).

Todas as empresas do Grupo CPFL tiveram que se adequar a SOX, que define a boa governança corporativa e as práticas éticas do negócio não mais como requinte, e sim como lei (MURATORE, 2012). Desde 2007, a RGE é certificada pelos critérios da Lei SOX, o que garante a integridade das demonstrações financeiras conforme regras e controles internacionais que são auditados periodicamente.

Nas auditorias, são feitas avaliações que testam e validam processos e controles internos. A SOX define uma maior transparência na divulgação das informações financeiras e dos atos da administração (MURATORE, 2012). É para garantir esta transparência que os sistemas são auditados periodicamente.

Para suportar uma eventual auditoria, uma mudança no ambiente de produção dos sistemas comerciais do Grupo CPFL deve ser acompanhada de evidências que comprovem que os pontos de controle da empresa foram atendidos.

Uma das iniciativas tomadas pela Governança de TI visando o atendimento dos pontos de controle encontrados na empresa foi a elaboração da MMS, um método estruturado para manutenção de SI da CPFL. Esta iniciativa demonstra que a governança de TI tem o intuído de estimular comportamentos desejáveis na utilização da TI, determinando quem sistematicamente toma as decisões e quem contribui para elas (WEILL e ROSS, 2006),

O *Control Objectives for Information and related Technology* (CobiT) explica que uma governança corporativa efetiva ajuda a garantir que o departamento de TI suporte os objetivos de negócio, otimiza os investimentos em TI e trabalha com os riscos e oportunidades relacionados a TI (COBIT, 2007).

No caso do Grupo CPFL, a equipe de Governança de TI, é responsável por verificar, adequar e automatizar processos e controles internos em todas as empresas do grupo, incluindo a RGE e seus sistemas.

As evidências controladas pela Governança de TI são criadas em momentos distintos do processo de atendimento de uma solicitação do usuário, envolvendo diferentes equipes, inclusive na etapa de passagem da alteração para o ambiente de produção.

A MMS, utilizada pela TI do Grupo, abrange o processo de mudança desde as possíveis formas de solicitações de alterações no sistema por parte dos usuários até a conclusão do atendimento delas.

O Grupo CPFL disponibiliza para todos os seus colaboradores um portal, chamado Portal de Serviços, onde o usuário pode fazer suas solicitações de alteração nos sistemas, seja em forma de demanda ou ocorrência. A partir destas solicitações são criadas as requisições de mudança em ambiente de produção.

Em 2013, foi iniciado pela CPFL um projeto chamado CCS RGE, que trata da migração do atual sistema Open-SGC para um novo sistema comercial, chamado *Customer Care and Services* (CCS).

O CCS é uma ferramenta comercial disponível no mercado de TI, já utilizada nas demais distribuidoras de energia elétrica do grupo CPFL. Com base neste sistema que foram elaboradas as metodologias MMSS (antiga) e MMS (atual).

Junto à implantação do sistema CCS para a RGE, também será implantada a MMS na empresa. Por ser uma migração do principal sistema utilizado, haverá uma grande mudança cultural, onde processos serão substituídos, outros serão alterados, e novos processos surgirão, estando estas situações já mapeadas nos riscos e impactos do projeto.

## 1.1 PROBLEMA DE PESQUISA

Não há um processo que demonstre como deve funcionar o registro de evidências durante o ciclo de vida de uma Requisição de Mudança (RDM) com a utilização da Metodologia de Manutenção de Sistemas (MMS) para suportar auditorias da SOX.

Como deve ser o processo de geração de evidências durante o ciclo de vida de uma RDM para que atenda as necessidades da CPFL e as boas práticas de auditoria?

## 1.2 OBJETIVOS

O objetivo geral deste trabalho de conclusão de curso é o desenvolvimento de um processo que mostre como deve ser a geração de evidências durante o ciclo de vida de uma RDM que atenda as necessidades da CPFL e as boas práticas de auditoria.

Para atingir este objetivo principal, seguem os seguintes objetivos específicos:

- Facilitar o entendimento do processo de geração de evidências durante o processo da RDM por parte da equipe de atendimento;
- Utilizar um procedimento único que represente o processo que possa ser utilizado pela Governança de TI da CPFL;
- Utilizar recursos da empresa que permitam a geração de evidências de forma que obedeçam as boas práticas de auditoria.

### 1.3 CONTRIBUIÇÃO CIENTÍFICA

As principais contribuições científicas deste trabalho são:

- Utilização de ferramentas automatizadas e que permitem a rastreabilidade para geração de evidências durante o ciclo de vida de uma RDM;
- Desenho de um processo em BPMN para complementação da metodologia de manutenção de sistemas do Grupo CPFL;
- A geração de evidências durante o ciclo de vida de uma solicitação de mudança para o ambiente de produção de um sistema que respeite as boas práticas de auditoria.

### 1.4 ESTRUTURA DO TRABALHO

O trabalho foi dividido em sete capítulos, objetivando um melhor entendimento de cada assunto abordado para a construção do novo processo.

O capítulo 2 apresenta os levantamentos bibliográficos, descrevendo os principais conceitos sobre auditoria, abordando técnicas e metodologias utilizadas quando da realização de uma auditoria, além de conceitos que afetam o resultado da auditoria na RGE. Estes conceitos são importantes pois o proposto neste trabalho deve atender eventuais auditorias na empresa.

O capítulo 3 fala sobre mudanças em SI, apresentando uma visão teórica da realização de mudanças, apresentando também pontos de controle envolvidos nesta atividade e conceitos da auditoria em mudanças em SI.

No capítulo 4 é apresentado o sistema comercial e a metodologia que serão implantados na RGE com o projeto CCS RGE, explicando como é o processo de mudanças em ambiente de produção no Grupo CPFL. Este capítulo apresenta ainda uma análise sumarizada do processo atual da empresa e uma descrição de problemas encontrados neste processo.

No capítulo 5 está descrita e desenhada em BPMN a proposta de solução elaborada para resolver o problema apresentado neste trabalho. Os passos de cada processo e subprocesso demonstram como devem ser realizadas as ações das equipes de atendimento de acordo com o processo proposto. Este capítulo apresenta também as diferenças encontradas entre o atual processo e o desenhado neste trabalho e uma seção sobre a orientação que deve

ser dada aos usuários envolvidos.

No capítulo 6 está detalhada a forma de teste e validação do processo criado utilizando o CRM Dynamics do Grupo CPFL, utilizando o plano de testes padrão do grupo em diferentes cenários de testes, levando em consideração os possíveis ciclos de vida de uma RDM.

O capítulo 7 apresenta a conclusão deste trabalho e propostas de melhorias futuras na CPFL. Após, constam as referências bibliográficas utilizadas para o embasamento teórico do trabalho e os anexos.

## 2 AUDITORIA

Entidades governamentais e privadas, independente do porte ou ramo de atividade, convivem e evoluem graças a uma quantidade cada vez maior de tecnologia. Desde 1950, segundo Imoniana (2008), mudanças ocorreram em todos os ambientes de negócio, onde empresas e instituições expandiram-se rapidamente.

Com este crescimento, os métodos de processamento de dados e sistemas de controles internos não conseguiram mais suprir a demanda organizacional, uma vez que os equipamentos começaram a expandir sua utilização em diversos setores das empresas.

Entretanto, os custos e o aumento de vulnerabilidade de sistemas emanados do uso de tecnologia de informação geraram a necessidade de auditores internos e independentes possuírem habilidades referentes a dados e sistemas, para garantir que acionistas, investidores, órgãos governamentais e demais usuários não se defrontem com situações incoerentes.

Nas próximas sessões são apresentados os principais conceitos relacionados a auditoria, análise de riscos, pontos de controle, metodologia de auditoria, coleta de evidências, metodologias de amostragem, comunicação em auditoria e a Lei SOX, que afeta diretamente o escopo da geração de evidências no processo de mudança na CPFL.

### 2.1 CONCEITUAÇÃO DE AUDITORIA

Conforme descrito por Stair e Reynolds (2006 apud BRANDALISE, 2012), SI são responsáveis por diversos papéis em uma empresa, onde coletam, processam, armazenam e distribuem informações destinadas a apoiar a tomada de decisões, análises e o gerenciamento das organizações. Segundo a definição de Gil (1999), “sistemas de informação compreendem um conjunto de recursos humanos, materiais, tecnológicos e financeiros, combinados segundo uma sequência lógica para transformar dados em informações”. Brandalise (2012) afirma ainda que, em empresas onde a TI é considerada parte do mapa estratégico, é importante que os seus SI estejam bem alinhados com os processos da própria organização.

As tecnologias presentes nas empresas são instrumentos que permitem a evolução empresarial e dão sustentação para que elas enfrentem e expandam o intenso entrelaçamento das tarefas de administração da organização moderna, graças à variedade de opções de emprego de tecnologia computacional em todas as áreas de uma empresa.

A auditoria, por sua vez, evoluiu e foi exigida, ultrapassando os seus limites originais de auditoria contábil e de auditoria tributária. A auditoria assumiu uma postura operacional, que atualmente é acompanhada da auditoria de SI, sendo esta, cada vez mais ampla, de acordo com o aumento da utilização de computadores (GIL, 1999).

A função da auditoria, segundo Lyra (2008), é promover adequação, revisão, avaliação e recomendações para o aprimoramento dos controles internos em SI, bem como, avaliar a utilização dos recursos envolvidos no processamento dos mesmos, atuando em todos os sistemas da organização, seja no nível operacional, tático ou estratégico.

Complementando, Brandalise (2012) afirma que a auditoria busca inovações, otimizações de processos empresariais, potenciais relações custo versus benefício, avaliação de riscos, maior eficiência, eficácia e segurança, tendo a empresa um meio de medir se seus resultados estão coerentes ou se podem ser melhorados.

Attie (2010) cita que o desempenho da auditoria requer a utilização de ferramentas de trabalho que permitam formar uma opinião, onde o objetivo da auditoria é fundamentar seu ponto de vista com fatos, evidências e informações possíveis, necessárias e materiais.

Attie (2010) afirma ainda que procedimentos de auditoria são as investigações que permitem a formação fundamentada da opinião do auditor sobre o trabalho realizado, sendo que o auditor, no momento de recolhimento e avaliação das evidências, necessita ser independente e imparcial, agindo com critério de forma isenta e inquestionável.

Quando aplicadas a TI, Imoniana (2008) afirma que as atividades de auditoria, além de tentar utilizar recursos de informática para auditar a própria tecnologia, também visam automatizar os processos de auditoria.

Em qualquer ramo, empresas que tem auditorias buscam diferencial no mercado. Para isso, no ponto de vista de Imoniana (2008), os objetivos para utilização de auditoria nas organizações são:

- Melhorar a eficiência e reduzir custos;
- Melhorar a qualidade do trabalho de auditoria, reduzindo níveis de risco;
- Atender às expectativas dos clientes;
- Preparar-se para a globalização dos negócios;
- Manter-se com bom conceito no mercado.

Nessa mesma linha, Jund (2002) cita que a auditoria de informática deve informar sobre:

- Adequação, eficácia, eficiência e desempenho dos sistemas e respectivos procedimentos de segurança;

- Custos relativos e economia no uso de investimentos dispendidos em processamento de dados;
- Segurança física: referente ao hardware da empresa;
- Segurança lógica: referente ao software da empresa.

A auditoria de SI, conforme Gil (1999) atua com a intenção de validar e avaliar o controle interno do ambiente computadorizado, podendo ser estudada a partir de três momentos:

- Auditoria de SI em operação normal;
- Auditoria durante o desenvolvimento de SI;
- Auditoria do centro de computação.

Segundo Lyra (2008), estes são os principais objetivos da auditoria em SI:

- Integridade: confiança nas transações processadas pelo sistema, pois o sistema garante a consistência das transações, onde o usuário pode embasar suas decisões sem receio;
- Confidencialidade: as informações são reveladas somente as pessoas que necessitam conhecê-las, havendo restrição de acesso a estas informações;
- Privacidade: as funções incompatíveis nos sistemas são segregadas, onde os usuários têm acesso somente àquelas informações necessárias à execução das suas tarefas;
- Acuracidade: as transações processadas podem ser validadas, onde há consistência de entrada de dados, atentando para a veracidade dos dados;
- Disponibilidade: o sistema deve estar disponível para o cumprimento dos objetivos da empresa, pois sua ausência pode representar problemas;
- Auditabilidade: os sistemas devem documentar *logs* operacionais que permitam que sejam realizadas trilhas de auditoria;
- Versatilidade: o sistema deve ser de fácil usabilidade por parte da empresa, se adaptando as necessidades da mesma;
- Manutenibilidade: políticas e procedimentos operacionais devem contemplar controles quanto a teste, conversão, implantação e documentação de sistemas, sejam novos ou modificados.

## 2.2 ANÁLISE DE RISCOS NO PROCESSO DE AUDITORIA

A análise de risco é um processo adotado para que o auditor saiba, com antecedência, quais são as ameaças no ambiente de uma organização. Segundo Imoniana (2008), estas ameaças constituem eventos futuros não desejáveis, cuja ocorrência resulta em problemas.

Complementando, Pizzoli (2004), explica que a análise de riscos abrange a identificação das ameaças e vulnerabilidades para os ativos cobertos pelo escopo da auditoria e seus possíveis impactos no negócio. A metodologia utilizada para elaboração dessa análise deve ser documentada, da mesma forma, os critérios para identificação dos riscos precisam ser registrados e inseridos na documentação da auditoria.

Conforme Imoniana (2008), a identificação de um risco em um sistema é provavelmente a tarefa mais difícil no processo de auditoria de sistemas, mas pode ser muito desastrosa caso as ameaças não sejam detectadas em tempo e brechas forem aproveitadas para acarretar um prejuízo financeiro para a organização.

A Associação Brasileira de Normas Técnicas (ABNT) apresenta a gestão de riscos com o objetivo de contribuir para (ABNT, 2008):

- Identificação dos riscos;
- Análise/avaliação dos riscos em função das consequências ao negócio e da probabilidade de sua ocorrência;
- Comunicação e entendimento da probabilidade e das consequências dos riscos;
- Estabelecimento da ordem prioritária para tratamento dos riscos;
- Priorização das ações para reduzir a ocorrência dos riscos;
- Envolvimento das partes interessadas quando as decisões de gestão de riscos são tomadas;
- Envolvimento das partes interessadas quanto à situação da gestão de riscos;
- Eficácia do monitoramento do tratamento dos riscos;
- Monitoramento e análise crítica regular de riscos e do processo de gestão de riscos;
- Coleta de informações de forma a melhorar a abordagem da gestão de riscos;
- Treinamento de pessoal a respeito dos riscos e das ações a mitigá-los.

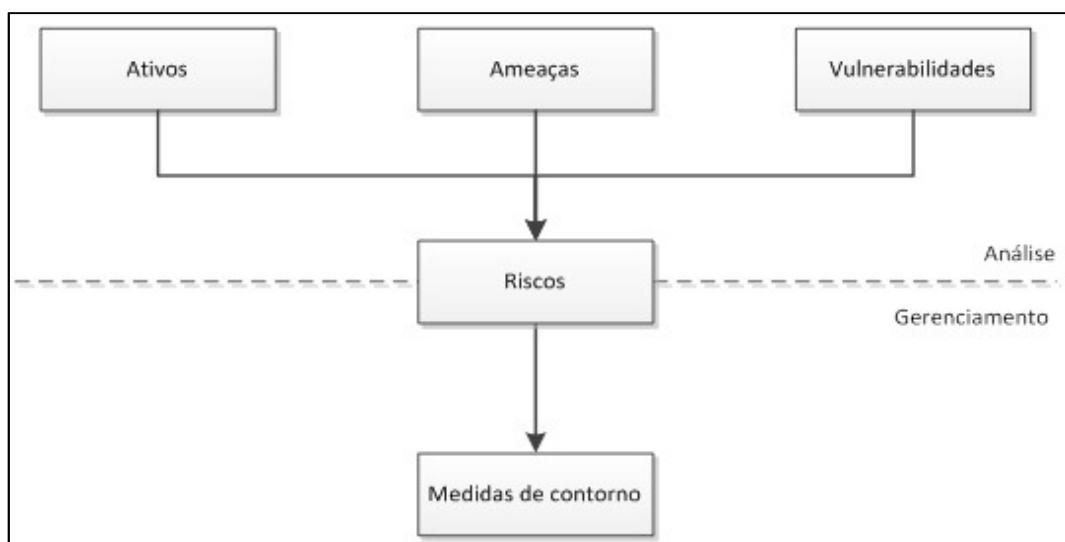
Para reduzir a ocorrência de riscos, e possibilitar a organização maior flexibilidade e competitividade na execução dos seus processos, Magalhães (2007) afirma que é necessário o gerenciamento e controle dos riscos. A gestão de riscos é importante para que as organizações

estejam atentas aos riscos que rondam o seu negócio, podendo garantir a sua segurança por já estarem preparadas para enfrentar possíveis ameaças.

Para o CobiT, segundo Fernandes (2006), a gestão de riscos é um dos pilares fundamentais que sustentam o núcleo da governança de TI, visando o conhecimento dos riscos por parte da alta direção, entendimento claro dos requisitos de *compliance*, transparência acerca dos riscos significativos para a empresa e incorporação de responsabilidades para o gerenciamento dos riscos na organização.

Segundo Magalhães (2007), a análise de risco divide-se em partes, as quais, isoladas representam muito pouco, mas, alinhadas e geridas de forma adequada, podem apontar caminhos seguros na busca do nível adequado de segurança para o negócio de uma organização. Conforme mostra a figura 1, a análise e o gerenciamento de riscos são atividades inter-relacionadas.

Figura 1 - Análise e gerenciamento de risco



Fonte: Adaptado de Magalhães (2007)

O processo de gestão de riscos, conforme a ABNT (2008) é composto por:

- Definição do contexto;
- Análise/avaliação de riscos;
- Tratamento do risco;
- Aceitação do risco;
- Comunicação do risco;
- Monitoramento e análise crítica de riscos.

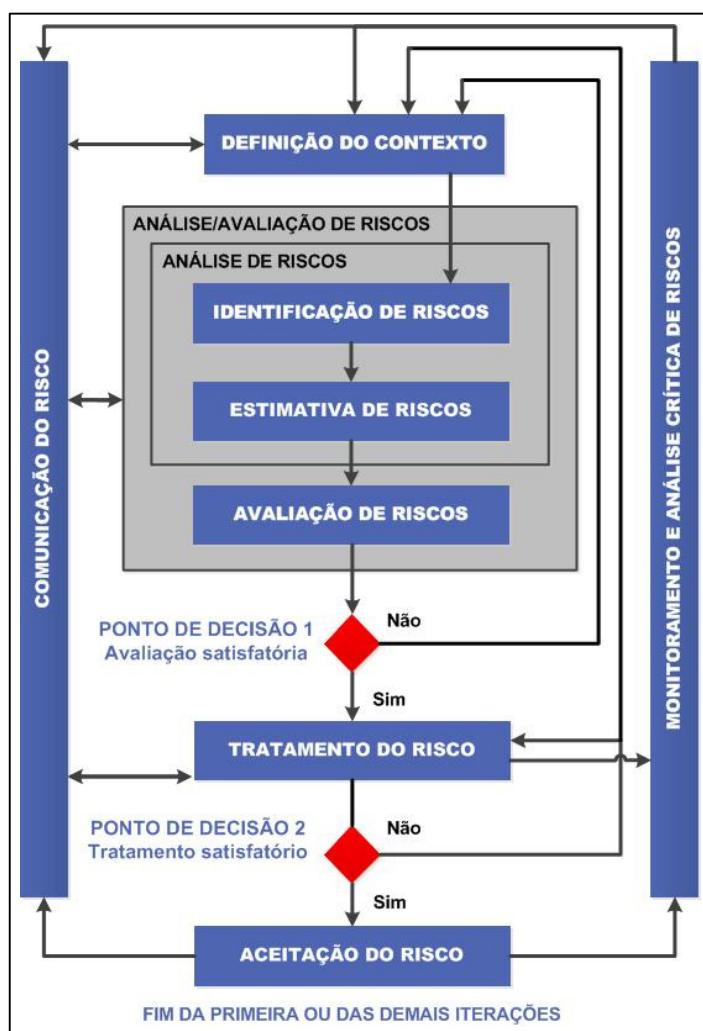
Conforme a definição do CobiT (2007), a gestão de riscos requer que os funcionários

mais experientes da organização tenham conhecimento a respeito do risco, que haja transparência sobre os riscos significantes para a organização e inserção do gerenciamento de riscos nas atividades da empresa.

Durante a gestão de riscos, a fase de análise/avaliação de riscos pode ser realizada mais de uma vez no processo. Um enfoque iterativo na execução da análise/avaliação de riscos torna possível aprofundar e detalhar a avaliação em cada repetição e permite minimizar o tempo e esforço despendidos na identificação de controles e ainda assegura que os riscos de alto impacto ou probabilidade possam ser adequadamente avaliados.

A figura 2 ilustra o processo de gestão de risco com suas etapas.

Figura 2 - Processo de gestão de riscos



Fonte: Adaptado de ABNT (2008)

A primeira etapa, chamada definição do contexto, seria o levantamento de informações do ambiente a ser implementada a gestão de riscos, incluindo a definição de critérios básicos

necessários para a gestão de segurança da informação, definição do escopo e dos limites, e o estabelecimento de uma organização apropriada para operar a gestão de riscos.

Após o contexto estar definido, executa-se a análise/avaliação de riscos com base nos dados levantados na etapa anterior. Conforme explica a ABNT (2008), é necessária a identificação de ativos, ameaças, controles existentes, vulnerabilidades e consequências para coletar dados para a atividade de estimativa de riscos. A etapa de identificação de riscos tem por objetivo determinar eventos que possam causar alguma perda potencial e deixar claro como, onde e porque a perda pode acontecer.

A análise de riscos pode ser empreendida com diferentes graus de detalhamento, dependendo da criticidade dos ativos, da extensão das vulnerabilidades conhecidas e dos incidentes anteriores envolvendo a organização. Conforme a ABNT (2008), uma metodologia para a estimativa de riscos pode ser qualitativa, quantitativa ou ainda uma combinação de ambas as formas.

A estimativa qualitativa é frequentemente utilizada inicialmente para obter uma indicação do nível de risco e revelar grandes riscos. Depois pode ser necessária uma realização de uma análise quantitativa ou mais específica nos grandes riscos. Estão incluídas na estimativa de riscos as etapas de avaliação de consequências, avaliação de probabilidades dos incidentes, e estimativa do nível de risco.

Para a avaliação dos riscos, é necessária uma lista dos riscos com níveis de valores designados e critérios para a avaliação de riscos, provenientes da estimativa de riscos. Na avaliação dos riscos são utilizados os critérios para avaliação definidos durante a definição do contexto.

Segundo a ABNT (2008), nesta etapa, o nível dos riscos deve ser comparado com os critérios de avaliação dos riscos e com os critérios para a aceitação do risco. Na avaliação, além dos riscos estimados, é importante considerar também os requisitos contratuais, legais e regulatórios. A norma da ABNT (2008) afirma ainda que “convém que os critérios de avaliação de riscos utilizados na tomada de decisões sejam consistentes com o contexto definido, relativo à gestão de riscos e levem em conta os objetivos da organização e o ponto de vista das partes interessadas”.

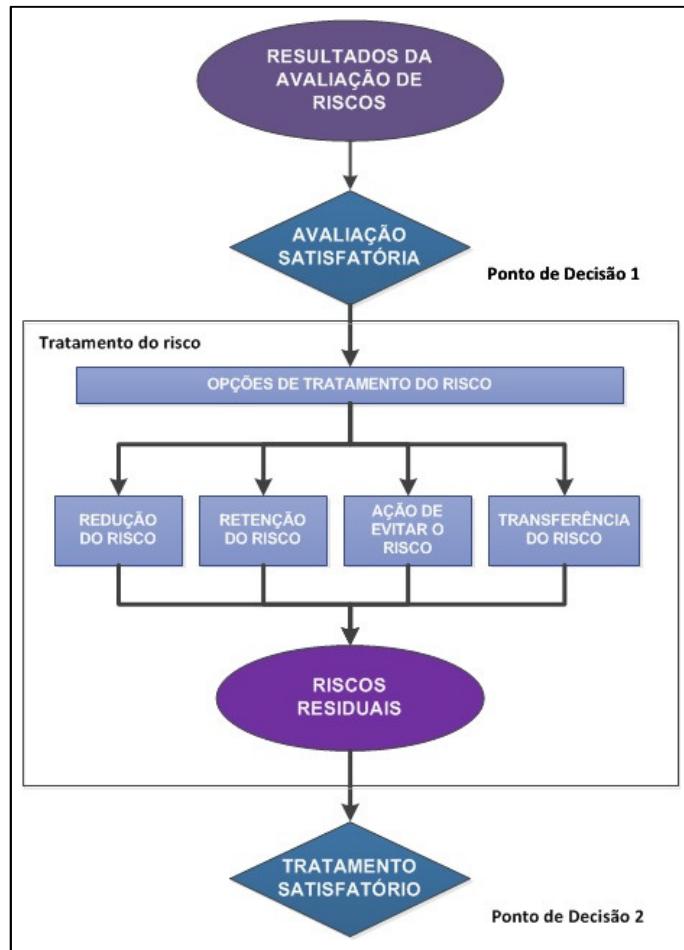
As decisões tomadas durante a avaliação de riscos são baseadas principalmente no nível do risco, porém, é importante que as consequências, probabilidade e grau de confiança na identificação e análise de riscos também sejam considerados.

Caso a análise disponha de informações suficientes para determinar de forma eficaz as ações necessárias para reduzir os riscos a um nível aceitável, a tarefa está concluída e pode-se

proceder com o tratamento do risco. Porém, se as informações coletadas na análise forem insuficientes, uma nova análise deve ser realizada, pois a eficácia do tratamento do risco depende dos resultados desta análise de riscos.

Há quatro opções disponíveis para tratamento de risco, que são redução do risco, retenção do risco, evitar o risco e transferência do risco, conforme ilustra a figura 3, que mostra os passos da atividade de tratamento do risco conforme a ABNT (2008).

Figura 3 - Atividade de tratamento do risco



Fonte: Adaptado de ABNT (2008)

As opções de tratamento de risco mostradas na figura 3 devem ser selecionadas com base no resultado da análise/avaliação de riscos, no custo esperado para implementação dessas opções e nos benefícios previstos. A ABNT (2008) afirma que quando uma grande redução do risco pode ser obtida com uma despesa relativamente baixa, as opções de tratamento devem ser implementadas. Caso as opções de melhorias sejam muito custosas para organização, uma análise precisa ser feita para verificar suas justificativas.

Quando o plano de tratamento do risco for determinado, precisam ser definidos os

riscos residuais. Para essa definição, pode ser necessária uma atualização ou uma repetição da análise/avaliação de riscos, considerando os efeitos previstos do tratamento que foi proposto. Caso o risco residual não satisfaça os critérios estabelecidos para a aceitação do risco, uma nova iteração do tratamento do risco pode ser necessária.

Na redução do risco, a intenção é que o nível de risco seja reduzido através da seleção de controles apropriados e devidamente justificados para que o risco residual possa ser reavaliado e então considerado aceitável. A escolha destes controles deve levar em consideração os critérios para a aceitação do risco, requisitos legais, requisitos regulatórios, requisitos contratuais, custos e prazos para a implementação de controles, além de aspectos técnicos, culturais e ambientais.

A opção de retenção de risco, sem outras ações adicionais, deve ser tomada tendo como base a avaliação de riscos. A retenção, consciente e objetiva por parte da organização, é uma opção desde que respeite as políticas da organização e os critérios para retenção do risco. Caso o nível do risco atenda aos critérios estipulados para retenção, não há necessidade de implementar controles adicionais e pode haver, então, a retenção do mesmo.

A ação de evitar o risco consiste em evitar a atividade ou condição que origina o determinado risco. Se os riscos forem considerados elevados e os custos da implementação de outras opções de tratamento de riscos excedam os benefícios que a organização pode ter, há a possibilidade de evitar o risco completamente. Para evitar o risco, pode-se optar por mudanças nas condições em que a operação ocorre ou através da eliminação de uma atividade planejada ou existente.

A transferência de risco envolve a decisão de compartilhar ou transferir determinados riscos com entidades externas, que possam gerenciá-lo de forma mais eficaz, dependendo da avaliação de riscos. Porém, esta transferência pode ocasionar novos riscos ou modificar riscos existentes e já identificados, podendo tornar necessário, um novo tratamento do risco.

Um seguro que cubra as consequências ou a contratação de um parceiro que seja responsável por monitorar o sistema de informação e tomar as medidas necessárias para evitar um dano ou prejuízo são alternativas para transferência de risco. Porém, a responsabilidade legal sobre as consequências, normalmente, não é transferível. Clientes podem atribuir a culpa de um efeito adverso diretamente à organização.

Em todos os momentos do processo pode ser realizada a comunicação de riscos, que consiste na troca ou compartilhamento de todas as informações sobre os riscos obtidas através da gestão de riscos entre o tomador de decisões e as outras partes interessadas (ABNT, 2008). Esta atividade tem por objetivo alcançar um consenso sobre como os riscos devem ser

gerenciados, com informações que incluam a existência, natureza, forma, probabilidade, severidade, tratamento e aceitabilidade dos riscos.

A norma da ABNT (2008) sobre a gestão de riscos afirma que o fruto desta etapa é um entendimento contínuo do processo de gestão de riscos na organização e dos resultados obtidos.

## 2.3 CONTROLES DE AUDITORIA

Lyra (2008) afirma que a informação é um bem cada dia mais valioso. Considerando um ativo de informação como “informação é tudo aquilo que a suporta e se utiliza dela”, e que ela pode possuir vulnerabilidades, é necessário concentrar esforços para mitigar riscos. Para tanto, Lyra (2008) define controle como todo e qualquer mecanismo utilizado para diminuir as vulnerabilidades de um ativo de informação, seja um equipamento, tecnologia, pessoa ou processo.

Conforme Brandalise (2012), programas de auditoria precisam ter um planejamento adequado e com objetivos definidos, pois assim o auditor consegue executar seus trabalhos chegando aos controles necessários, agregando técnicas de auditoria para auxílio em suas análises e constatações. Quando um auditor tem conhecimento sobre o ambiente e dos seus controles, provavelmente tenha um melhor desempenho nas suas responsabilidades dentro do programa de auditoria.

Segundo Lyra (2008), os pontos de controle podem ser encontrados nos documentos de entrada, relatórios, telas, arquivos, bancos de dados, pontos de integração e demais elementos relevantes para o sistema. Conforme Imoniana (2008) existem diversos tipos de controles em SI, desde formais até os informais, dependendo a sofisticação do sistema em operação.

Segundo Guimarães (2010), é necessário ficar claro que alguns tipos de falhas ou riscos existentes nas organizações sofrem ações de fatores externos que só podem ser identificados após o acontecimento destes. Somente após isso se pode criar uma sequência lógica para que os controles atendam as expectativas obtidas quando os mesmos foram desenhados.

Há restrições que podem afetar a seleção de controles (Exemplo: financeiras, técnicas, operacionais, culturais e éticas). Tais restrições podem dificultar a utilização de certos controles ou induzir a erros, podendo chegar à anulação do controle, a dar uma falsa sensação de segurança ou tornar o risco maior do que seria sem o controle.

Guimarães (2010) apresenta o conceito de controles organizacionais. Segundo ele, o controle organizacional é um conjunto de métodos e ferramentas que a empresa utiliza para manter-se na trajetória para alcançar os seus objetivos. No ponto de vista de Imoniana (2008), controles organizacionais são os controles administrativos instalados nos processos de fluxo das transações econômicas e financeiras dos SI, que auxiliam na consecução dos objetivos de negócio.

Os controles organizacionais são responsáveis, entre outros pontos, por (IMONIANA, 2008):

- Delineamento das responsabilidades operacionais;
- Coordenação de orçamento de capital de informática e bases;
- Desenvolvimento e implementação das políticas globais de informática;
- Intermediação com terceiros.

Em geral, os controles podem fornecer um ou mais tipos de proteção, que são correção, eliminação, prevenção, minimização do impacto, dissuasão, detecção, recuperação, monitoramento e conscientização. Para a seleção de controles, deve-se levar em conta o custo da aquisição, implementação, administração, operação, monitoramento e manutenção dos controles em relação ao valor dos ativos sendo protegidos.

Segundo Guimarães (2010), os controles organizacionais de uma empresa, a fim de trabalhar de melhor forma os processos existentes, também podem ser divididos, tendo os controles internos como parte deste universo. O CobiT (2007) define o controle interno como políticas, planos e procedimentos e a estrutura organizacional criada para prover uma razoável certeza de que os objetivos de negócio serão atingidos e eventos indesejáveis serão impedidos e corrigidos.

Os controles internos, segundo Attie (2010), algumas vezes são confundidos com auditoria interna. Mas, isso é um equívoco, uma vez que auditoria interna equivale a um trabalho organizado de revisão e apreciação dos controles internos, que por sua vez, se referem a procedimentos de organização adotados como planos permanentes da empresa. Conforme Gil (1999), a área de auditoria, seja ela interna ou externa, deve realizar a validação e avaliação de controles internos de SI.

Complementando, Imoniana (2008) afirma que os controles internos representam a coordenação de um conjunto de métodos e medidas adotados em uma empresa a fim de manter o ativo, verificar a exatidão e a veracidade dos registros, promover a efetividade do sistema de informação e fomentar uma grande adesão às políticas da empresa.

Jund (2002) afirma que quanto melhores e mais eficientes os controles internos

implantados na empresa auditada, mais segurança adquire o auditor com relação aos exames que está realizando. Conforme Jund (2002) essa eficiência é também fator de economia do tempo a ser empregado pelo auditor no seu trabalho e redução do custo da auditoria. Guimarães (2010) complementa explicando que para que os controles internos dos processos sejam efetivos, se faz necessário auditá-los a fim de aprimorá-los para resultados eficientes.

Imoniana (2008) classifica os controles internos em controles administrativos, controles de segurança e privacidade, controles de preparação e captação de dados, controles de entrada de dados, controles de processamento, controles de saída e de emissão de relatórios, e controle de gravação e recuperação de dados.

Na definição de Guimarães (2010), quando um controle é criado, ele pode ser preventivo, detectivo e corretivo:

- Controle preventivo: é o que tem mais importância, pois desempenha uma espécie de mapa para a execução do processo prevenindo a futura ocorrência de problemas. Para isso, se faz necessário a criação de controles que ajudem a identificar possíveis riscos;
- Controle detectivo: se tratam de procedimentos de controle adicionais que informam à administração que a eficiência operacional e a adesão às diretrizes gerenciais prescritas estão sendo alcançadas;
- Controle corretivo: tem o objetivo de corrigir problemas descobertos pelos controles detectivos. Incluem procedimentos que identifiquem a causa dos problemas, corrigir dificuldades ou erros, da mesma forma, modificar o sistema da empresa para que ocorrências futuras do problema sejam eliminadas ou minimizadas.

## 2.4 TÉCNICAS DE COLETA DE EVIDÊNCIAS

Conforme Brandalise (2012), para realização das atividades do ambiente a ser auditado, é importante que o auditor de SI tenha conhecimento do que tratam os pontos de controle. Isso porque estes serão os principais meios para obtenção de evidências durante todo o processo de auditoria.

Uma evidência de auditoria é um registro, depoimento, documento ou qualquer observação que comprove a ocorrência, ou não, de determinada atividade, fornecido pelo auditado para reforçar uma afirmação feita ao auditor. Chen; Smiliauskas; Trippen (2007)

afirmam ainda que a evidência é a base para justificar qualquer conclusão da auditoria, sendo fundamental para o processo de auditoria.

Na execução dos trabalhos de auditoria de SI, Imoniana (2008) afirma que técnicas convencionais, como questionários, indagação corroborativa, observação, exames documentais e da reexecução de tarefas, podem ser aplicadas para a obtenção de evidências.

Para auditar as informações de um ambiente de TI, segundo Imoniana (2008), o auditor pode desenhar a abordagem que lhe convir, levando com consideração a sofisticação do sistema computadorizado e características do próprio auditor. São as abordagens mais conhecidas:

- Abordagem ao redor do computador: Auditoria de documentos-fonte, com funções de entrada subjacentes e dominando as funções de saída, que se encontram em formatos de linguagem legível por leigos em informática, onde pouca atenção é dada às funções de processamento. É baseada na asserção de que os *inputs* de sistemas podem ser tidos como corretos se os resultados do sistema refletirem com precisão os dados-fonte. Então o *output* também deve ser correto e as formas pelas quais o sistema processou os dados têm pouca consequência;
- Abordagem através do computador: Este método alerta quanto ao manuseio de dados, aprovação e registro de transações comerciais, sem deixar evidências documentais razoáveis através de controles de programas construídos junto aos sistemas. Nesta, o auditor precisa acompanhar o processamento através e dentro do computador. Para isso, o auditor precisa de conhecimento quanto ao processamento de dados;
- Abordagem com o computador: é um meio de auditar as tecnologias com a maior perfeição possível, utilizando uma abordagem completamente assistida. Compila-se o processo, utilizando capacidades lógicas e aritméticas do computador para verificar se os cálculos são feitos corretamente, e utiliza-se a capacidade matemática para analisar e fornecer listas de amostras de auditoria.

As evidências são obtidas durante a etapa de execução dos procedimentos de auditoria, com o intuito de confirmar os conhecimentos a respeito dos sistemas operacionais, administrativos e financeiros, bem como, os seus procedimentos de controle. Jund (2002) afirma ainda que as evidências coletadas devem ser medidas por suficiência, pertinência e fidedignidade.

Complementando, Gil (1999) propõe ainda a alternativa de realização da técnica de

visita *in loco* como ferramenta de coleta de evidências para uma auditoria em TI. Desta forma, o auditor assiste a coleta das evidências, junto a sistemas, procedimentos e instalações do ambiente computadorizado.

O auditor deve obter evidências de auditoria que sejam suficientes, pertinentes e fidedignas para fundamentar suas conclusões, devendo elas fazer parte dos seus papéis de trabalho. Tais evidências podem ser de diferentes classes. Jund (2002) explica as classes de evidências da seguinte forma:

- Evidência física: é obtida pela comprovação da existência de instalações, recursos humanos, imóveis, equipamentos, veículos, móveis, utensílios, ou ainda, realização de obras e serviços;
- Evidência documental: consiste em registros, contratos, relatórios, faturas, recibos, documentos e/ou formulários. São três as suas categorias mais importantes, as quais proporcionam distintos graus de confiabilidade ao auditor:
  - Evidências documentais produzidas e mantidas por terceiros;
  - Evidências documentais produzidas por terceiros e mantidas em poder da organização;
  - Evidências documentais produzidas e mantidas pela entidade;
- Evidência analítica: se trata de análises que devem ser registradas nos papéis de trabalho do auditor ou na própria cópia do documento analisado, desde que a mesma seja incorporada no dossiê de auditoria;
- Evidência testemunhal: quando a evidência se trata de informações obtidas de pessoas que tenham conhecimento dentro e fora da organização auditada, em forma de declaração recebida em respostas a perguntas formuladas por escrito;
- Evidência por confirmação de terceiros: consiste na corroboração por escrito de terceiros em relação a determinadas informações, sendo aplicável, principalmente, a fornecedores, prestadores de serviço, bancos e clientes. Quando obtida através de fontes independentes externas a empresa, proporciona maior segurança para fins de auditoria do que as que foram obtidas exclusivamente dentro da empresa.

Nessa mesma linha, Imoniana (2008) afirma que a fase de evidenciação deve abranger a definição dos relatórios que serão gerados, a descrição do processo executado e dos resultados, e as conclusões de auditoria e emissão de relatórios.

Attie (2010) afirma ainda que a qualidade dos sistemas de informações da empresa

deve permitir ao auditor avaliar o grau de controle sobre as operações da empresa. Isso porque, se um administrador recebe informações resumidas, não tem condições de identificar os problemas ou tendências adversas em atividades específicas. Os responsáveis de cada área devem ter informações de sua respectiva área, senão o auditor deve estender a auditoria até alcançar informações que a própria área não possui.

## 2.5 CONTROLE DE ACESSOS

Segundo Lyra (2008), para se ter segurança em um ambiente lógico, é necessário se preocupar com a autenticação dos usuários e com a restrição do acesso dos usuários aos serviços autorizados. Nessa mesma linha, Imoniana (2005) afirma que as atividades de controle de acesso lógicas às informações, softwares e dados são atribuídas a políticas de segurança de informações bem estruturadas.

Durante o processo de geração de evidências de uma RDM, a autenticação dos usuários é importante para permitir a rastreabilidade da origem dos dados presentes no sistema, sabendo-se quem inseriu ou modificou qualquer dado consultado.

Quanto à autenticação de usuários, Lyra (2008) afirma que em geral, para a identificação de usuários com acesso a recursos computacionais, são criadas contas de usuários com uma identificação única, utilizando-se um método de autenticação para verificar esta identidade:

- O que você sabe: baseado na senha de acesso que o usuário possui, havendo uma política de troca de senhas ou bloqueio por inatividade;
- O que você tem: baseado em algo que o usuário tenha consigo, como um cartão magnético ou cartão com chip;
- O que você é: baseado em características físicas do usuário, como o reconhecimento facial ou impressão digital.

Estas senhas devem estar sujeitas a processos formais e rotineiros de concessão e alteração. Imoniana (2005) afirma ainda que o uso de senhas e números de identificação é um controle efetivo em um sistema para prevenir acesso sem as devidas autorizações.

Sobre a restrição de acesso dos usuários aos serviços que lhe são autorizados, Lyra (2008) explica que realizar uma administração adequada dos privilégios concedidos aos usuários dos SI baseada no uso de procedimentos rotineiros e formais, protege os ativos da informação contra acessos não autorizados. É importante que após a autenticação do usuário,

o mesmo só consiga acessar os dados que tiver privilégio para acessar.

Para obter melhores resultados na segregação de acessos aos usuários, Imoniana (2005) recomenda a aquisição e implementação de sistemas de segurança de informação, que devem ser customizados para atender as políticas de segurança de informação de cada organização.

## 2.6 LEI SARBANES-OXLEY

A missão básica da auditoria, conforme Jund (2002) é assessorar a administração no desempenho de suas funções e responsabilidades. Uma delas é a realização de um exame da integridade e confiabilidade dos sistemas estabelecidos para assegurar a observância de políticas, metas, planos, procedimentos, leis, normas e regulamentos, tal como, a efetiva utilização destes sistemas.

Jund (2002) afirma que a auditoria oferece para a área fiscal da empresa uma vantagem: contribui para maior observância das leis fiscais. Logo, conclui-se que no processo de auditoria, são sempre consideradas as leis que afetam a organização.

No caso da empresa RGE a lei diretamente envolvida no processo de auditoria é a Lei SOX. Isso porque a empresa faz parte do Grupo CPFL, que tem capital aberto e ações listadas na bolsa de valores norte-americana, e assim sendo, a obediência à Lei SOX é obrigatória (MURATORE, 2012).

Em 30 de julho de 2002, o então presidente George W. Bush assinou a Lei SOX e a apresentou ao conhecimento dos líderes empresariais e funcionários do governo no mundo inteiro. Conforme Souza (2004), a lei proíbe, por exemplo, que novos empréstimos sejam concedidos a conselheiros e executivos de empresas abertas.

Souza (2004) afirma que a lei é a mais importante mudança na legislação no mercado americano desde a criação das bases da lei atual, em 1933-1934. A lei aumentou o grau de responsabilidade desde o presidente e a diretoria da empresa até as auditorias e advogados contratados. Souza (2004) afirma ainda que, no caso das empresas brasileiras, o maior conflito é o que trata do comitê de auditoria.

Com as rígidas exigências da Lei SOX nos controles internos das empresas, surgiram uma série de oportunidades de negócios para as empresas de TI, que lançaram uma série de serviços para atender as necessidades das companhias na área de gerenciamento de riscos, arquivamento de documentos e segurança de informações (SOUZA, 2004).

Conforme Peters (2007), para que as empresas estejam em conformidade com a Lei,

grandes mudanças foram necessárias para se atender a seção 404 do capítulo IV – Ampliação de Divulgações Financeiras, que determina uma avaliação anual dos controles e procedimentos internos para a emissão de relatórios financeiros.

A seção 404 define, entre outros itens, que um auditor independente deve emitir um relatório distinto que confirme a asserção da administração sobre a eficácia dos controles internos e dos procedimentos executados para emissão dos relatórios financeiros.

Resumidamente, entre outros, a resolução define (PETERS, 2007):

- Implantação e implementação de controles internos voltados para as atividades desenvolvidas pelas organizações, seus sistemas de informações financeiros, operacionais e gerenciais e o cumprimento das normas legais e regulamentares a elas aplicáveis;
- Os controles internos devem prever a segregação das atividades de forma que seja evitado o conflito de interesses, a contínua avaliação dos diversos riscos associados às atividades da organização e o acompanhamento sistemático das atividades desenvolvidas, de forma a assegurar que quaisquer desvios possam ser corrigidos.

A tabela 1 mostra as implicações operacionais da Lei SOX para o departamento de TI de uma empresa.

Tabela 1 - Implicações da Lei para TI

(continua)

<b>Requisitos de qualidade da informação</b>	<b>Implicações da Lei SOX</b>
O conteúdo da informação deve ser apropriado	Processo de desenvolvimento de requisitos de software; Processo de gerenciamento de requisitos de software; Métodos de engenharia de software; Processos de testes; Processos de homologação; Processo de gestão da mudança e da configuração.
A informação deve estar disponível no momento em que for necessária	Disponibilidade de aplicativos; Disponibilidade de infraestrutura; Gerenciamento de incidentes e problemas no ambiente de produção; Gestão de aplicativos e de ativos de TI; Gerenciamento de disponibilidade e desempenho.

(conclusão)

<b>Requisitos de qualidade da informação</b>	<b>Implicações da Lei SOX</b>
Os dados e as informações estão corretos	Segurança da informação em aplicativos; Teste de software; Controle da mudança e da configuração; Gerenciamento de dados; Gerenciamento de requisitos.
A informação é acessível aos usuários interessados	Segurança da informação referente ao controle de acessos e privilégios; Controle de autorizações.
Sistema de controle interno sobre relatórios financeiros	Avaliação de riscos de TI; Gestão da qualidade; Planos de desastres e recuperação.

Fonte: Adaptado de Fernandes (2006)

## 2.7 CONSIDERAÇÕES FINAIS

Neste capítulo foi apresentada a definição de auditoria e conceitos, técnicas e procedimentos necessários para compreender o contexto no qual é útil o processo de geração de evidências que devem acompanhar uma RDM, juntamente com conceitos sobre gestão de acessos e sobre a Lei SOX.

Para a elaboração de um processo que complemente a metodologia MMS utilizada no grupo CPFL serão considerados os conceitos de controles de auditoria, técnicas de coleta de evidências e o estudo sobre a Lei SOX apresentados neste capítulo.

Conforme consta no CobiT (2007), uma vez que os objetivos estejam definidos, eles precisam ser monitorados para assegurar que atendam às expectativas. Para tanto, no processo proposto serão aplicados conceitos que fundamentem a geração de evidências durante o ciclo de vida das mudanças, fornecendo a base necessária para as atividades de auditoria.

As evidências registradas no processo podem ser documentais, analíticas ou testemunhais, conforme explicado por Jund (2002). Tais evidências devem atender ao que está requisitado na seção 404 da Lei SOX, cujas empresas de auditoria externa solicitam a coleta de tais evidências para suas avaliações com uma abordagem através do computador, apresentada por Imoniana (2008).

Uma auditoria, quando em mudanças de SI, tem o papel de promover a adequação,

avaliação e apresentação de recomendações para o aprimoramento de controle interno nos SI de uma empresa (LYRA, 2008). Logo, para definição do processo proposto, o próximo capítulo apresenta conceitos de mudanças em SI.

### **3 MUDANÇAS EM SISTEMAS DE INFORMAÇÃO**

Novos sistemas precisam ser colocados em operação, uma vez que esteja concluído o seu desenvolvimento. É necessária a realização de testes apropriados em um ambiente dedicado, definição de instruções de implantação e migração, planejamento de liberação de mudanças no ambiente produtivo e uma revisão pós-implementação. Isso assegura que os sistemas estejam alinhados com as expectativas e resultados acordados (COBIT, 2007).

As funções de desenvolvimento e implantação de SI, no ponto de vista de Imoniana (2008) devem ser atribuídas a indivíduos que tenham competências para conceber e implantar sistemas. Naturalmente, há envolvimento dos usuários com o propósito de atender aos objetivos da área de negócio, cumprindo obrigações da área de desenvolvimento de sistemas e garantindo as funções de pós-implantação de sistemas.

É importante a participação do auditor desde o início do desenvolvimento de SI ou do processo de seleção para aquisição, pois desta forma, é possível recomendar o aperfeiçoamento dos controles internos ainda no início, evitando modificações no sistema depois de pronto.

Nas próximas sessões são apresentados conceitos relacionados a implantação de SI, pontos de controle presentes na implantação de SI e sobre a auditoria na etapa de implantação de mudanças em SI, importantes para a contextualização de uma mudança em SI, processo em que devem ser geradas corretamente as evidências.

#### **3.1 IMPLANTAÇÃO DE MUDANÇAS EM SI**

Conforme Imoniana (2008), normalmente, quando novos sistemas ou modificações significativas em sistemas existentes são colocados em produção, o risco de erros relacionados a transações processadas por esses sistemas pode ser aumentado.

Tendo em vista o controle das mudanças de TI, Magalhães (2007) apresenta o processo de gerenciamento de mudança, um dos gerenciamentos que faz parte da *Information Technology Infrastructure Library* (ITIL).

O gerenciamento proposto por Magalhães (2007) visa controlar quaisquer mudanças que possam impactar os níveis de serviços acordados com as áreas de negócio de maneira processual, documentada e controlada, objetivando o mínimo de impactos negativos.

O gerenciamento de mudança tem o objetivo de agir como um processo de planejamento e controle. O processo do ITIL abrange itens como:

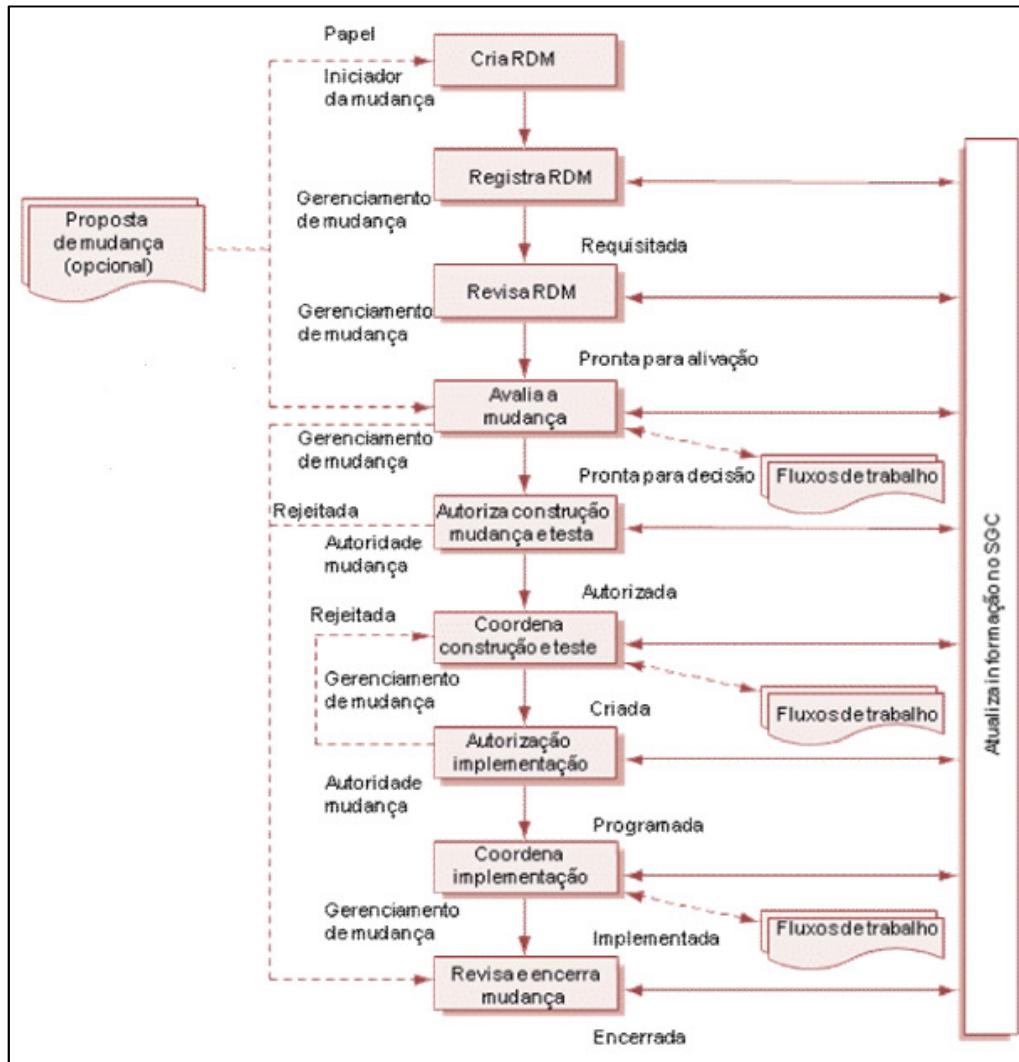
- Softwares aplicativos e sistema operacional;
- Sistemas de negócio;
- Pacotes comerciais e bancos de dados;
- Relacionamento entre bancos de dados, aplicações e links entre sistemas;
- Versões do software.

Segundo Neto (2012), para realizar as mudanças de forma proposta no gerenciamento de mudança, é necessária uma avaliação dos riscos, impactos e do processo de aprovação de mudanças. A aprovação de mudanças deve ser realizada por um grupo responsável pela avaliação e aprovação das mudanças, constituído por profissionais de TI e representantes da área de negócio.

Os benefícios da utilização da gestão de mudança do ITIL, segundo Lorandi (2009) são: redução do impacto negativo da mudança, controle maior da execução da mudança e conforme a necessidade do negócio, mudanças filtradas e priorizadas.

A figura 4 apresenta um fluxograma mostrando os passos propostos pelo ITIL para um ciclo de vida de uma RDM (LORANDI, 2009), onde aparecem todos os passos que deve passar a RDM, sendo que em todos os passos pode haver uma atualização de informações para com o sistema de gerenciamento de conhecimento, onde devem ficar os registros para uma base de conhecimento.

Figura 4 - Fluxograma proposto para uma mudança



Fonte: Adaptado de Lorandi (2009)

O gerenciamento de mudanças em serviços de TI do ITIL prevê planos de retorno para o caso de mudanças que não possam ser concluídas por algum motivo, sendo estas informações todas registradas (NETO, 2012). Mudanças nos SI podem ter um impacto negativo devido à interrupção do serviço, para isso o gerenciamento de mudanças define entre outros pontos:

- Priorizar e responder para a área de negócio sobre as mudanças;
- Contribuir para as exigências da governança, exigências legais, contratuais e regulatórias;
- Reduzir as mudanças falhas e consequentemente interrupção do serviço, defeitos e retrabalho;
- Entregar as mudanças de acordo com tempo e necessidade do negócio;
- Avaliar os riscos associados com a transição de serviços;

- Trabalha em conjunto com a área de negócio para oportunidades de melhoria para organização.

Complementando, o CobiT (2007) afirma que um gerenciamento de mudanças insatisfatório poderia prejudicar a confiança depositada em testes de integridade por parte da organização.

Todas as mudanças solicitadas, incluindo manutenções e correções de emergência realizadas nos sistemas no ambiente de produção, devem ser gerenciadas formalmente e de maneira controlada.

As mudanças devem ser registradas, avaliadas, autorizadas antes da implementação e revisadas em seguida, tendo como base os resultados efetivos e planejado, assegurando a mitigação de riscos e impactos negativos na estabilidade ou na integridade do ambiente de produção (COBIT, 2007).

### 3.2 PONTOS DE CONTROLE EM MUDANÇAS DE SI

Conforme o CobiT (2007), os controles presentes na implantação de mudanças para o ambiente de produção são:

- Padrões e procedimentos de mudança: estabelecer procedimentos formais de gerenciamento de mudanças para haver um padrão em todas as solicitações de mudança em aplicações, procedimentos, processos, parâmetros de serviço e plataformas subjacentes;
- Avaliação de impacto, priorização e autorização: avaliar todas as solicitações de mudança de modo estruturado com relação a impactos no sistema operacional e na respectiva funcionalidade. Todas as mudanças devem ser categorizadas, priorizadas e autorizadas;
- Acompanhamento de status e relatórios de mudanças: estabelecer um sistema de acompanhamento e relatórios de mudanças para controlar mudanças rejeitadas, comunicar status de mudanças aprovadas e em andamento. Deve-se garantir que as mudanças autorizadas sejam implementadas conforme planejado;
- Finalização da mudança e documentação: atualizar a documentação, os procedimentos do sistema e de usuários sempre que forem implementadas mudanças no sistema.

No ponto de vista de Lorandi (2009), o processo de gerenciamento de mudanças abordado no ITIL está representado na figura 5.

Figura 5 - Gerenciamento de Mudanças



Fonte: Adaptado de Lorandi (2009)

No modelo apresentado por Lorandi (2009), as RDMs e a Programação Futura de Mudanças (PFM) são as principais entradas do processo, que tem como saída, Requisições de mudanças aprovadas, atas de reunião do conselho e informações gerenciais do processo.

Com a adoção do modelo proposto por Lorandi (2009), todas as implementações e alterações em TI são analisadas e planejadas para que se tenha o menor risco e impacto. Os benefícios são redução do impacto negativo da mudança, controle maior na execução da mudança e execução conforme necessidade da área de negócio.

### 3.3 AUDITORIA DE MUDANÇAS EM SI

Segundo Gil (1999), as principais análises que devem ser feitas na auditoria do desenvolvimento de sistemas computadorizados são da metodologia de desenvolvimento de sistemas e da documentação do desenvolvimento de sistemas.

Complementando, a *Information System Audit and Control Association* (ISACA), reforça a necessidade da metodologia, pois é necessário um procedimento padrão para a execução e registro das alterações realizadas nos sistemas, que deve incluir medidas para garantir que as mudanças sejam devidamente autorizadas, testadas e documentadas (ISACA, 2011).

Segundo Imoniana (2005), a documentação de um sistema de informação é um conjunto de documentos que apoiam e explicam aplicações dos programas, devendo orientar sobre o funcionamento destes. Os documentos são importantes não somente para os analistas de sistemas, mas também para usuários, equipe de gestão de acessos, empregados novos, auditores, programadores e equipe de futuros projetos.

A ISACA (2011) afirma ainda que é importante que todos os documentos relevantes do sistema sejam atualizados, o que é muitas vezes negligenciado devido a limitações de tempo e recurso. O objetivo é manter uma coerência interna entre o sistema e seus fluxogramas, dicionários de dados, modelos de relacionamento de entidades, diagramas, procedimentos da operação e manuais do usuário final.

Sobre a auditoria em mudanças em SI, a ISACA (2011) fala sobre a importância de um formulário padrão para a solicitação da RDM. Conforme Imoniana (2005), as auditorias devem verificar se as requisições de alterações nos programas seguem as orientações utilizadas na empresa, não resultando na implementação de programas inadequados ou não autorizados.

Mudanças não autorizadas, conforme Imoniana (2005), não devem ser implementadas em ambiente de produção. Ele recomenda ainda que a TI tenha formas de rastrear, talvez por comparação de versões, se acontecem estas modificações indevidas. Sistemas específicos podem ser utilizados para ajudar neste controle. Nessa mesma linha, a ISACA (2011) alerta que uma alteração não autorizada pode ocorrer por problemas de comunicação entre a equipe, onde a mudança não foi analisada/aprovada conforme previsto, o código fonte alterado não foi revisado pelos responsáveis, ou ainda pode ter uma alteração do programador feita no código em benefício próprio.

Também existem as mudanças emergenciais que, segundo a ISACA (2011), devem ser um ponto de atenção especial dos auditores. Mudanças emergenciais podem ser necessárias para resolver problemas do sistema e permitir que continue seu processamento em produção. A equipe de operação e os analistas de sistemas devem seguir um procedimento específico para esta situação, sem comprometer desnecessariamente a integridade/disponibilidade de nenhum componente do sistema além do que já está com problema.

### 3.4 CONSIDERAÇÕES FINAIS

Neste capítulo foram apresentados conceitos sobre a implantação de SI, os controles existentes neste procedimento, incluindo o uso de referências consolidadas aplicáveis a gestão

de mudanças (CobiT e ITIL) e conceitos sobre auditorias que envolvam mudanças em SI, incluindo referências da ISACA.

O CobiT é uma referência por ser baseado na análise e harmonização dos padrões e boas práticas de TI existentes que age como um integrador das práticas de governança de TI e influencia direção, gerências, profissionais de governança e de auditoria de TI (COBIT, 2007).

O ITIL, por sua vez, é uma estrutura de trabalho conhecida mundialmente para o gerenciamento de serviços de TI, baseado no ciclo de vida de serviço em diferentes níveis, incluindo o gerenciamento de mudança e o gerenciamento de liberação e implantação (LORANDI, 2009).

A ISACA é uma associação que é fonte de conhecimento, padrões, relacionamento e desenvolvimento de carreira para auditores de SI, segurança, risco, privacidade e profissionais de governança de TI (ISACA, 2011).

De modo geral, o processo de geração de evidências deverá respeitar os passos descritos na documentação de sistemas existente no Gerenciamento Eletrônico de Documentos (GED) do Grupo CPFL quanto a procedimentos realizados pelas equipes de TI e orientar sobre a geração de evidências adequadas às atividades de auditoria.

O ambiente de sistemas no qual o processo proposto foi desenhado segue descrito no próximo capítulo, mostrando pontos que são positivos e negativos.

## 4 PROCESSO ATUAL NA CPFL

O Grupo CPFL, da mesma forma que outras empresas, implementou a Governança de TI tendo em vista que a tomada de decisões sobre TI não deve ser considerada menos importante do que em outras áreas da organização. Weill; Ross (2006) afirmam que empresas com clareza e foco em TI geralmente produzem resultados melhores em qualquer empreendimento.

No caso da CPFL, a equipe de governança de TI é responsável pelos controles de TI em todas as empresas do grupo, que atuam em geração, transmissão e distribuição de energia elétrica em diferentes estados e com diferentes sistemas. Para não haver divergência entre estratégias e procedimentos, a TI de todas as empresas se mantém alinhada com a equipe de governança, que acompanha a execução dos processos, faz os contatos necessários e trabalha nas auditorias realizadas.

Para as auditorias, o Grupo CPFL tem em seu GED o Regulamento de Auditoria do Grupo CPFL (GED 13135), onde afirma que a auditoria auxilia a organização a alcançar seus objetivos adotando uma abordagem sistemática e disciplinada para a avaliação e melhoria da eficácia dos processos de gerenciamento de riscos, de controle e governança corporativa.

O GED CPFL é um repositório padrão da empresa para arquivamento de documentos. Ele está disponível na intranet para todos os colaboradores da empresa em suas estações de trabalho, podendo ser acessado por todos os analistas de negócios, de sistemas e de operação do grupo. Este alinhamento permite ter transparência sobre a governança de TI. Weill; Ross (2006) explicam que, quanto maior for a transparência dos processos de governança, maior será a confiança na governança.

Na RGE, a MMS, que define regras gerais para conduzir os ciclos de manutenção de sistemas, começou a ser utilizada desde que as ferramentas utilizadas para atendimento das solicitações dos usuários foram alinhadas.

Conforme descrito na própria MMS, ela consolida e simplifica boas práticas e recomendações de mercado, incluindo *Capability Maturity Model Integration* (CMMI), *Interactive Development* e *Agile Development*.

A MMS é utilizada pela equipe responsável pelos sistemas comerciais no atendimento de ocorrências e demandas abertas pelos usuários da RGE referentes ao sistema Open-SGC, atualmente, sistema comercial utilizado pela empresa.

Este capítulo tem por objetivo apresentar o sistema comercial utilizado pelo grupo

CPFL, a metodologia de manutenção de sistemas utilizada, o procedimento realizado no ciclo de vida da RDM, uma análise sumarizada do processo atual e os problemas encontrados no processo que é atualmente realizado.

#### 4.1 SISTEMA COMERCIAL DA RGE

Desde o ano 2000, a RGE utiliza o Open-SGC como sistema comercial, onde são realizadas as suas operações comerciais, desde o cadastro de um cliente, até o faturamento de seu consumo de energia, aplicando diversos conceitos do negócio de energia elétrica entre estas duas operações.

Mas, visando o alinhamento de sistemas, a CPFL iniciou o Projeto CCS RGE, com o propósito de migrar os dados da RGE para este novo sistema, liberar licenças para todos os usuários e mudar os processos e sistemas satélites utilizados na RGE.

Um dos objetivos do projeto é alinhar a RGE na utilização do sistema CCS, desenvolvido pela *Systeme, Anwendung und Programme* (SAP), e demais ferramentas utilizadas pelas outras distribuidoras de energia elétrica do grupo.

A ferramenta foi desenhada para empresas de serviços públicos, permitindo, de forma flexível, a criação de pedido de leitura de contadores, produção de ordens de serviço em contadores, faturamento, entre outras ações.

O CCS na CPFL tem os seguintes módulos:

- Serviço de Campo;
- Perdas;
- Gestão de Ativos;
- Gestão de Leitura;
- Atendimento ao Cliente;
- Faturamento;
- Arrecadação e Cobrança Contábil, Fiscal, Financeiro e Inadimplência.

Além disso, o sistema CCS se comunica com outros sistemas através de uma interface construída para receber e enviar informações com os seus sistemas satélites. Esses sistemas podem ser outras ferramentas utilizadas no grupo, sistemas web ou equipamentos móveis, auxiliando a empresa em adquirir agilidade e precisão nos dados.

## 4.2 METODOLOGIA MMS

Segundo a ISACA (2011), para o controle da manutenção evolutiva contínua de um sistema, é necessário um processo padrão para a execução e registro das alterações. Nessa mesma linha, conforme seção 3.2, o COBIT (2007) reforça a importância de se estabelecer um procedimento padrão para o gerenciamento de mudanças.

O procedimento utilizado na RGE é a MMS e está publicado no GED CPFL, documento 14085. Seu objetivo é estabelecer um método estruturado para manutenção de SI, incluindo práticas, recomendações e controles para tratar as demandas e a implantação das mudanças, sendo aplicada às manutenções de sistemas que estão em produção no Grupo CPFL.

A metodologia permite sua adaptação e aplicação aos diversos sistemas e tecnologias presentes nas empresas do grupo, bem como a integração e equivalência de diversos métodos técnicos quando vindo de provedores de serviços externos de desenvolvimento de sistemas, integrados a cadeia de valor de TI.

As solicitações de alterações nos SI geradas pela área de negócio são atendidas através de uma ferramenta da Microsoft utilizada pelo grupo chamada *Customer Relationship Management (CRM) Dynamics*. As solicitações são abertas com focos diferentes: manutenção evolutiva e manutenção corretiva.

Quando a manutenção é chamada Evolutiva, é porque trata da adição de novas funcionalidades ao sistema, ou ainda, alterações nas funcionalidades já existentes a fim de atender mudanças nos requisitos do sistema ou atender alguma nova legislação.

Para tanto, a forma de solicitação de alteração a ser criada pelo usuário é uma demanda, que deve impreterivelmente ter as seguintes etapas:

- O usuário-chave da área de negócio deve abrir a demanda no Portal de Serviços;
- A demanda deve ser aprovada pelo gestor imediato do usuário-chave;
- O usuário-chave deve encaminhar um documento com a especificação funcional da sua solicitação;
- A demanda passa por uma análise de viabilidade técnica e estimativa de esforço (custo e prazo) por parte da equipe que irá atendê-la;
- A demanda deve ser priorizada entre área de negócio e a gestão de TI, com base no tipo e custo da demanda, tendo prioridade demandas legais (originadas por solicitações regulatórias);

- A demanda terá um cronograma que será mantido atualizado pelo analista responsável pelo atendimento;
- Quanto ao desenvolvimento, cabe à equipe responsável gerar seus próprios artefatos, mantendo-os anexos na demanda no próprio CRM Dynamics;
- Para homologação deve ser criado um plano de testes, onde serão incluídos os testes realizados, o resultado obtido, as evidências da realização destes testes e o aceite do usuário;
- A aprovação pode ser feita via CRM Dynamics ou e-mail, desde que permita posterior rastreabilidade.

As mudanças corretivas devem ser originadas com uma alegação de erro no sistema ou anormalidade. Esta solicitação é chamada Ocorrência, cuja manutenção a ser realizada tem o objetivo de sanar o problema encontrado no sistema.

Mudanças corretivas podem ser também situações em que os usuários precisam resolver questões do dia-a-dia de trabalho, onde alterações devem ser realizadas via banco de dados por não ser possíveis via aplicação.

Há três diferentes situações para solução da manutenção corretiva:

- Na avaliação do analista responsável, a solução do problema pode ser feita dentro do prazo esperado, então ele deve resolver o problema, liberar o uso da ferramenta, informar a solução implantada, solucionar a ocorrência e ajustar a documentação da base de conhecimento;
- Na avaliação do analista responsável, a solução não pode ser feita dentro do prazo estipulado no CRM Dynamics, mas existe uma forma de contornar o problema, então ele deve aplicar a solução paliativa, liberar o uso da funcionalidade do sistema, informar a solução implantada e abrir um Registro de Problema, para que a solução definitiva seja desenvolvida, solucionando a ocorrência;
- Na avaliação do analista responsável, a solução do problema não pode ser realizada dentro do prazo e não há forma de contornar o problema, então ele deve comunicar ao seu superior imediato e ao usuário informando o prazo para resolução do problema, para então trabalhar na solução, corrigir o erro, liberar o uso da funcionalidade do sistema, informar a solução implantada, solucionar a ocorrência e ajustar a respectiva documentação na base de conhecimento, se aplicável.

Em muitos dos casos atendidos, principalmente de manutenção evolutiva, a conclusão

do atendimento necessita de uma RDM. As RDMs devem ser sempre registradas no CRM Dynamics, ferramenta utilizada pelo grupo CPFL para gestão das ocorrências e demandas abertas pelos usuários da área de negócio no Portal de Serviços.

### 4.3 REQUISIÇÃO DE MUDANÇA

O processo da RDM tem como objetivo controlar a avaliação de impacto, autorização e implantação de mudanças na infraestrutura e nas aplicações evitando inconsistência e indisponibilidade dos sistemas, conforme sugerido pelo COBIT (2007) na seção 3.1.

Para implantação de mudanças no ambiente de produção é necessário o controle de avaliação de impacto, priorização e autorização. Neste sentido, está correto o procedimento adotado, pois tais as mudanças já são avaliadas e previamente autorizadas, em conformidade com a orientação do COBIT (2007) na seção 3.2.

Segundo a metodologia utilizada, o ciclo de vida da RDM é o seguinte:

- A requisição da mudança é aberta formalmente no CRM Dynamics;
- A RDM deve passar por uma análise de risco e impacto;
- A RDM deve ser aprovada por um responsável na TI;
- A mudança é executada conforme planejamento técnico;
- A RDM deve ser finalizada conforme o sucesso ou não da execução.

Porém, estes passos são abrangentes, não descrevendo exatamente como ocorre uma RDM. Esta etapa, de forma geral, prevê as regras para migração para produção das manutenções preparadas para os sistemas a sua validação final pelos solicitantes.

O sistema CCS tem sua manutenção realizada por uma equipe que trabalha com a linguagem *Advanced Business Application Programming* (ABAP). Esta é a linguagem de programação utilizada pela empresa SAP no desenvolvimento do CCS.

As mudanças a serem efetuadas no ambiente de TI necessitam de uma requisição formal. Logo, o analista de sistemas responsável por atender a solicitação do usuário, após a homologação, para realizar uma alteração em base de produção, abre uma RDM na ferramenta CRM Dynamics.

No caso do CCS, primeiramente as alterações são realizadas em um ambiente próprio para desenvolvimento, onde são realizadas as alterações em interface, regras de negócio e/ou configurações funcionais necessárias para atender a necessidade do usuário. Estas alterações são testadas pela equipe de desenvolvimento neste ambiente até que se tenha um resultado

positivo.

Após a conclusão dos testes no ambiente de desenvolvimento, a equipe faz a transferência das alterações para um ambiente específico para homologações. Esta mudança é realizada pela própria equipe de desenvolvimento. Para isto, o ABAP gera uma requisição, que é um arquivo com todas as alterações realizadas, identificado por um número, posteriormente utilizado nas mudanças para o ambiente de produção. Este procedimento está de acordo com as orientações da ISACA (2011), que afirma primeiramente as alterações devem ser desenvolvidas e exaustivamente testadas em um ambiente apropriado, para somente após isto serem transportadas para o ambiente de produção.

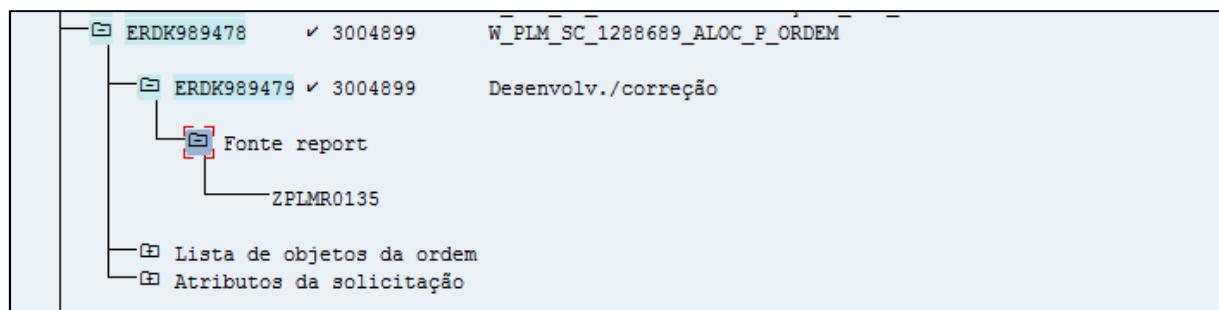
Depois de homologadas pelos usuários, as alterações são transportadas a partir de uma RDM do ambiente de homologação para o ambiente de produção. A RDM é registrada no CRM Dynamics para formalização, onde as evidências são incluídas. Importante salientar que, por regra, não se consegue transportar mudanças para produção sem uma requisição.

A RDM é, portanto, um meio por onde são formalizadas as mudanças a serem realizadas no ambiente de produção, conforme solicitado pelo usuário, com um número de requisição e as evidências necessárias para uma possível auditoria.

Conforme a ISACA (2011), o formulário da RDM deve incluir, no mínimo, o nome do solicitante (Solicitante), data do pedido (Data de Criação), data em que é necessária a mudança (Data Prevista de Implementação), prioridade do pedido (Prioridade), descrição da solicitação de mudança (Descrição da Solução), descrição dos efeitos previstos em outros sistemas (Sistemas Afetados com a Mudança) e procedimento de retorno (Plano de Retorno). O usuário pode ainda informar a razão para a mudança (Descrição do Problema) e os benefícios esperados (Descrição do Impacto).

A figura 6 apresenta uma requisição utilizada no CCS, onde aparece o objeto alterado, que é o ZPLMR0135, que foi modificado pelo analista de sistemas com matrícula 3004899. As requisições são identificadas por um código que é incluído na RDM para ser transportada.

Figura 6 - Exemplo de uma requisição utilizada no CCS



Fonte: Elaborado pelo autor

Para melhor entender o processo, uma alternativa é desenhá-lo em uma notação clara e objetiva. Segundo Tessari (2008), uma notação padrão para modelagem de negócios pode prover para as empresas a capacidade de entender os seus procedimentos internos de negócio de forma gráfica e dar a habilidade de comunicar estes procedimentos de modo padrão. Além disso, a notação gráfica facilita o entendimento das colaborações e as transações de negócio entre as organizações, permitindo que as empresas se entendam e também os participantes em seu negócio.

A BPMN (*Business Process Modeling Notation*) é uma notação que tem como propósito a geração de um diagrama de processos de negócio através de um conjunto básico de elementos gráficos. Estes elementos permitem o desenvolvimento de diagramas que são, normalmente, bastante familiares para a maioria dos analistas de negócio, pois são bastante parecidos com fluxogramas (WHITE, 2004 apud TESSARI, 2008).

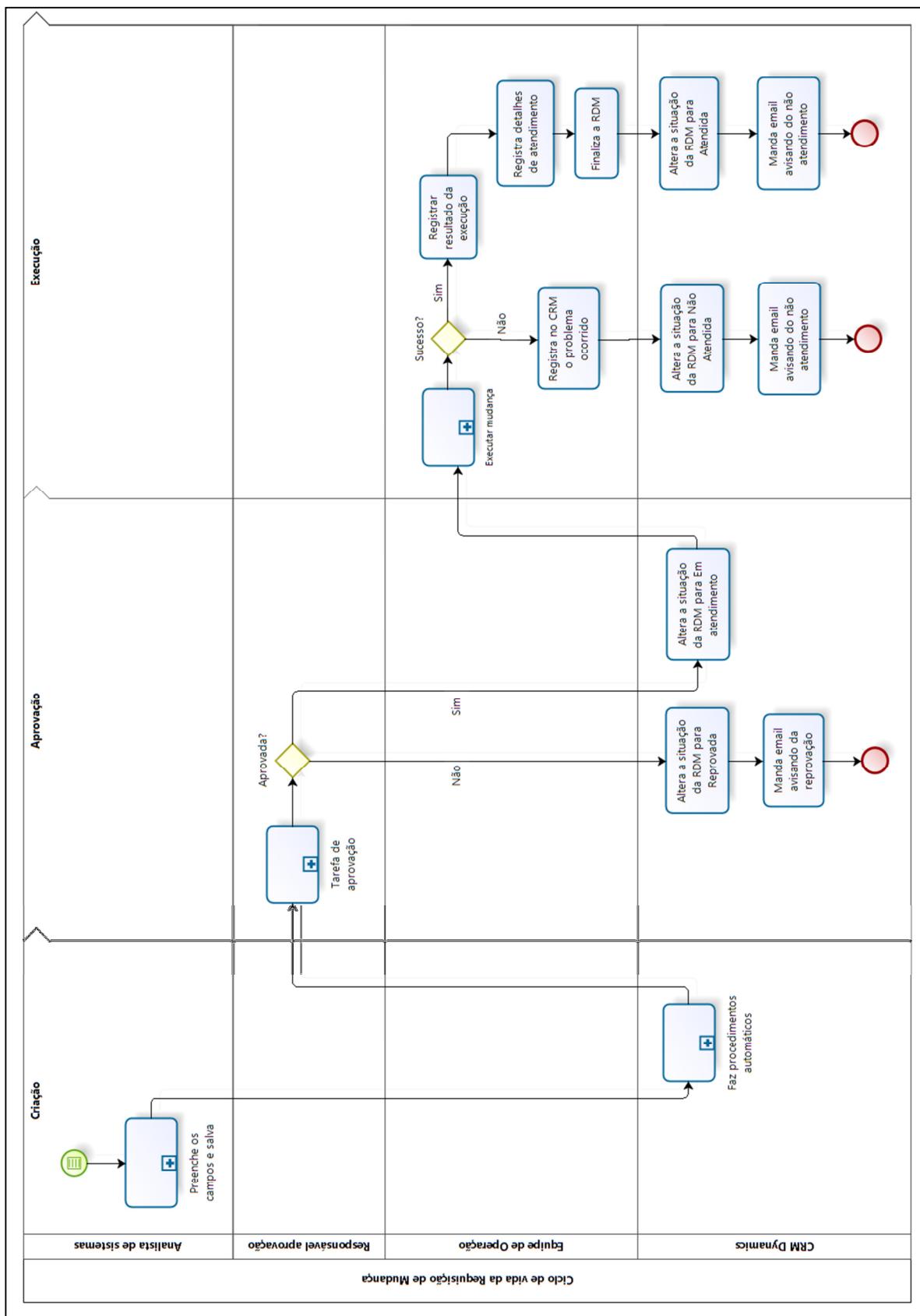
Entre abrir uma RDM, atender e encerrar, o processo contém uma série de passos que deve ser executada por diferentes usuários no CRM Dynamics. Conforme a ISACA (2011), a segregação de funções e responsabilidades, de atividades e tarefas e a restrição dos dados por usuário, são princípios da garantia no processo de auditoria.

Para o ciclo de vida da RDM, o CRM Dynamics tem diferentes perfis para cada um dos atores envolvidos. Estes perfis limitam os acessos dos usuários ao que é necessário a sua função, obedecendo aos objetivos de auditoria privacidade e confidencialidade, apresentados por Lyra (2008).

A metodologia presente na CPFL apresenta três fases da RDM (criação, aprovação e execução), tendo a participação de três atores principais (analista de sistemas, responsável pela aprovação e equipe de operação), fora o próprio CRM Dynamics. Esta divisão de responsabilidade entre diferentes atores é uma orientação da ISACA (2011), que sugere que os acessos devem ser restritos, sendo que somente um grupo de operadores, qualidade ou ainda um grupo de controle de mudanças deve executá-las.

O ciclo de vida da RDM na CPFL já tem alguns pontos em comum com o ITIL, apresentado na seção 3.1. Tais pontos em comum são: criação da RDM em uma ferramenta de gestão de mudanças, preenchimento de campos de impacto e risco, análise de risco e impacto da mudança, aprovação da mudança. A figura 7 ilustra o processo atual da RDM em BPMN.

Figura 7 - Processo da RDM em BPMN



Fonte: Elaborado pelo autor

### 4.3.1 Criação da RDM

A RDM é criada no CRM Dynamics a partir de uma solicitação formal de um usuário da área de negócio, que pode ser nas formas descritas na seção 4.2. Este vínculo é necessário pois não se deve fazer uma alteração no sistema que não venha de uma solicitação da área de negócio.

A origem de uma RDM por ser a partir de:

- Uma demanda, na aba “Detalhes” acessar “Gestão de Mudanças Relacionada” e após em “Novo”, na janela “Pesquisar Registro”;
- Uma ocorrência, na aba “Detalhes” acessar “Mudança Relacionada” e após em “Novo”, na janela “Pesquisar Registro”;
- Um registro de problema, na aba “Geral” acessar “RDM” e após em “Novo”, na janela “Pesquisar Registro”.

A ISACA (2011) recomenda que as RDMs sejam abertas por um sistema de gerenciamento de mudanças, seguindo um formulário padrão. No caso da CPFL, a RDM segue o formulário do CRM Dynamics.

A figura 8 apresenta a tela apresentada pelo CRM Dynamics para a criação de uma nova RDM.

Figura 8 - Janela Pesquisar Registro

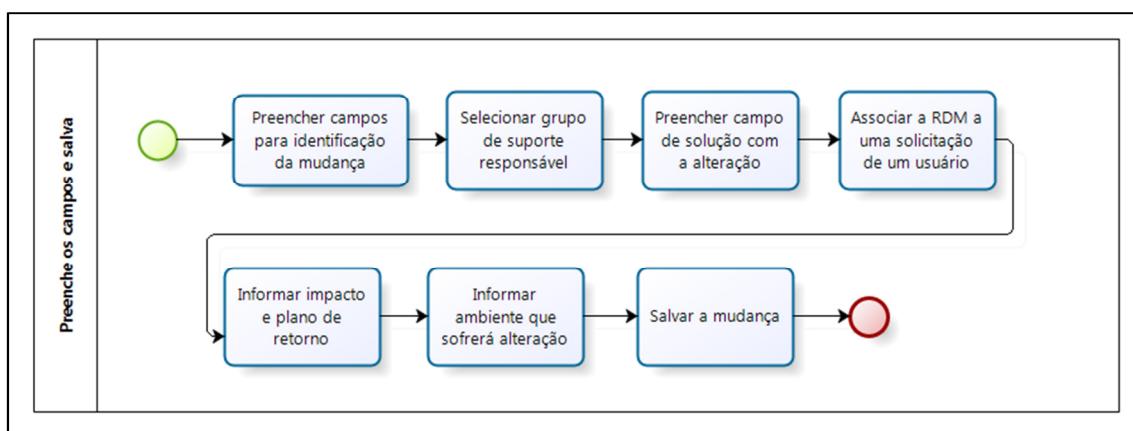
Título	Id da Mudança	Data de Criação
! Atualizar Base Qualidade - CS	RDM-006068	22/08/2011 10:17
! Cadastrar e executar o programa ZCCSGLER0082 com ...	RDM-0022995	11/09/2013 17:17
! Erro no Pase diario cancelou programa DWBI_PL_0010...	RDM-0020763	20/06/2013 11:17

Fonte: Microsoft Dynamics CRM (2011)

Neste momento, o CRM Dynamics abre a janela da nova RDM. Quanto mais campos forem preenchidos, menores são os riscos de haver algum problema na execução da RDM. Os campos sinalizados nesta janela com asterisco são os de preenchimento obrigatório, devendo ser preenchidos pelo analista de sistemas.

A figura 9 ilustra o primeiro subprocesso da figura 8, com os passos do processo de preenchimento de uma RDM, explicados no decorrer da seção.

Figura 9 - Início do preenchimento dos dados na criação



Fonte: Elaborado pelo autor

Conforme a ISACA (2011), o formulário da RDM deve incluir no mínimo, no nome do solicitante (Solicitante), data do pedido (Data de Criação), descrição da solicitação da mudança (Descrição da Solução) e a razão para mudança (Descrição do Problema), presentes no CRM Dynamics.

A figura 10 apresenta os campos iniciais da aba “Geral”. Estes são os primeiros campos a serem preenchidos em uma RDM, sendo que alguns deles são pelo analista de sistemas e outros pelo próprio CRM Dynamics.

Figura 10 - Informações básicas da RDM

**Geral**

**Informações básicas da Mudança**

Id da Mudança	Situação *	Nova
Data de Criação	Proprietário *	LEONARDO PAIM
Solicitante *	Grupo de Suporte *	
Mudança *		
Descrição do Problema *		
Descrição da Solução *		
Riscos Associados		
Origem da RDM	Gestão de Mudanças	
Demandas Relacionadas		
Ocorrências		
Registro de Problemas		

Fonte: Microsoft Dynamics CRM (2011)

O campo “Id da Mudança” será preenchido automaticamente pelo CRM Dynamics no momento que a mudança for salva pelo número que identifica a RDM. Este número é a principal forma de localização desta mudança.

O campo situação não é alterado pelo usuário, somente pela própria aplicação CRM Dynamics. Este campo é importante, pois esclarece em que situação está a RDM, sendo este o campo que aparece nos relatórios da governança.

O campo data de criação é de preenchimento automático do CRM Dynamics, mostrando o momento de sua criação. Nas auditorias, este campo é parâmetro para definir se a RDM vai para a amostra ou não, já que estas são delimitadas em períodos.

No campo “Proprietário” deve ser inserido o nome do usuário que irá atender a mudança. No momento que o CRM Dynamics gera o número da mudança, preenche este campo com um usuário default, proprietário do assunto inserido.

O campo “Solicitante” se refere ao analista que está solicitando a mudança, que é o responsável por ela, tendo que responder caso haja algum problema na execução ou falte alguma evidência se esta mudança estiver na amostra selecionada pela equipe de auditoria.

O campo “Grupo de Suporte” deve conter o nome da equipe responsável por colocar a mudança no ambiente desejado, que no caso do CCS é a TI\_SAPCCS\_Basis. Desta forma, a RDM constará na fila de atendimento desta equipe.

No campo “Mudança” é preenchido o título, que é uma referência ao que será realizado, facilitando a identificação da mudança posteriormente.

A descrição do problema é o local onde deve ser descrito o que será resolvido com a implantação da referida mudança. Enquanto que, a descrição da solução se trata da solução que será dada ao problema através da mudança a ser realizada.

O campo “Riscos Associados” deve ser preenchido com os riscos encontrados através de uma análise realizada pelo solicitante quanto à mudança que está realizando no ambiente.

O campo “Origem da RDM” é um campo de preenchimento do próprio CRM Dynamics, não sendo alterado pelos usuários, que reflete a forma como foi originada a RDM.

Os campos “Demanda Relacionada”, “Ocorrência” e “Registro de Problemas” são os campos onde o analista de sistema solicitante pode preencher com o número identificador da solicitação que está atendendo da área de negócios.

Após os dados iniciais, o usuário tem os campos opcionais da Documentação para preencher. Estes campos, não são utilizados pela equipe de manutenção de sistemas.

Os campos de informações para priorização são utilizados pela equipe de Operação para priorização do que deve ser atendido, devido ao grande número de RDMs recebidas pelas equipes diariamente. Dentre estes campos, há a data em que é necessária a mudança (Data Prevista de Implementação), prioridade do pedido (Prioridade) e procedimento de retorno (Plano de Retorno) e os benefícios esperados (Descrição do Impacto), que são campos vistos como essenciais em uma RDM pela ISACA (2011).

A figura 11 apresenta a etapa de Informações para Priorização.

Figura 11 - Informações para priorização na RDM

Informações para priorização	
Impacto *	<input type="text"/>
Data Prevista de Implementação	<input type="text"/> <input type="button" value="..."/>
Motivo *	<input type="text"/>
Serviço Datacenter	<input type="text"/> <input type="button" value="..."/>
Plano de Retorno *	<input type="text"/>
Descrição do Impacto *	<input type="text"/>
Prioridade	<input type="text"/>
Assunto *	<input type="text"/> <input type="button" value="..."/>
Mudança Emergencial?	<input checked="" type="radio"/> Não <input type="radio"/> Sim

Fonte: Microsoft Dynamics CRM (2011)

Nos campos de impacto e prioridade deve ser selecionada uma das opções (alto, baixo ou médio), dependendo de cada RDM, levando em consideração uma avaliação técnica sobre a alteração a ser realizada pelo solicitante.

O campo de data prevista de implementação só é ocupado em casos em que há um agendamento prévio da execução da RDM.

O campo “Assunto” deve ser preenchido com o mesmo assunto da solicitação aberta pelo usuário da área de negócios no portal de serviços. Este campo é utilizado nos relatórios da governança para avaliar quais os assuntos das mudanças que estão sendo atendidas.

No campo referente a motivo é sinalizado porque mudança é necessária, que pode ser desde solucionar um incidente ou aplicar uma melhoria funcional no sistema.

A opção de mudança emergencial é utilizada para alertar os envolvidos que a RDM deve ser atendida com prioridade. Este campo pode ser selecionado após a criação da RDM, basta selecionar a opção “Sim” e salvar novamente. Mas este recurso, por orientação da gerência de TI, não deve ser utilizado, pois já houveram problemas devido a atendimentos emergenciais (sem autorização prévia) que posteriormente não foram autorizados e a RDM ficou sem esta evidência.

O campo de RDM Emergencial, como outros da RDM, não é solicitado, por exemplo, pela CISA ou pela SOX. Da mesma forma que outros campos presentes no formulário da RDM, este não é utilizado pelas equipes envolvidas na manutenção do sistema comercial, porém, como outros sistemas também têm a sua manutenção feita também através do CRM Dynamics Dynamics, tais campos são necessários para outras equipes.

O campo “Serviço Datacenter” é utilizado somente pela equipe de operação e em casos de mudanças que envolvem infraestrutura de TI, não interferindo no processo de auditoria de sistemas.

O plano de retorno deve conter as principais ações para reestabelecer o ambiente caso haja algum problema na execução da RDM. Este procedimento está de acordo com as orientações de Neto (2012) na seção 3.1. No caso de necessidade de retorno, o analista de sistemas solicitante pode ser contatado para verificar o que deve ser feito com a RDM.

O campo “Descrição do Impacto” descreve qual o impacto que o ambiente irá sofrer com a execução da RDM, através de uma análise técnica realizada pelo analista de sistemas solicitante da mudança.

A próxima seção da RDM tem as informações cronológicas (aprovações) e o campo item de configuração. As informações cronológicas são preenchidas pelo próprio CRM Dynamics no decorrer dos trâmites da RDM, apresentando quando e por quem a RDM foi aprovada, e o campo item de configuração, que não é utilizado pela equipe de manutenção de sistemas.

A figura 12 ilustra os campos de informações cronológicas (Aprovações) e o item de configuração na RDM.

Figura 12 - Informações cronológicas e de configuração na RDM

The screenshot shows a form titled "Informações cronológicas (Aprovações)". It contains fields for "Aprovador 1", "Aprovador 2", and "Aprovador Emergencial", each with a lookup icon. To the right, there are two sets of date fields: "Data de Aprovação 1" and "Data de Aprovação 2", and "Data de Aprovação Emergencial", each with a calendar icon. Below these is a radio button group for "RDM Aprovada?" with options "Não" (No) and "Sim" (Yes). The next section, "Item de configuração", contains a field labeled "IC" with a lookup icon.

Fonte: Microsoft Dynamics CRM (2011)

Nos campos de implementação, devem ser informados os servidores envolvidos na mudança e quais SI serão afetados com a mudança. Os analistas podem ainda preencher os campos de duração prevista e tempo de indisponibilidade, facilitando o trabalho da equipe de operação em organizar seus cronogramas de atividades.

A figura 13 apresenta os campos de informações técnicas e banco de dados na RDM. Nesta etapa da RDM está o campo com a descrição dos efeitos previstos em outros sistemas (sistemas Afetados com a Mudança), conforme sugerido pela ISACA (2011).

Figura 13 - Informações para implementação da RDM

Fonte: Microsoft Dynamics CRM (2011)

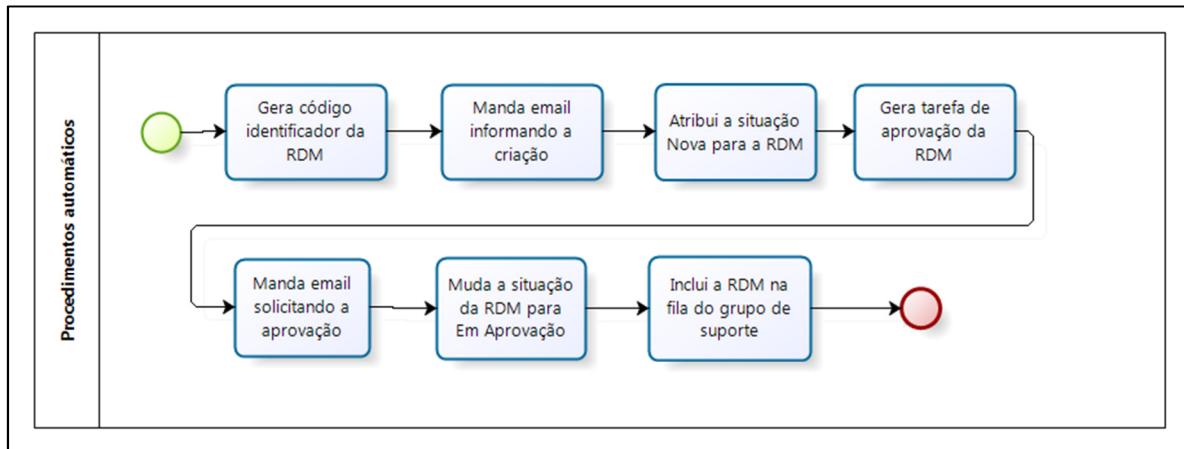
As informações de banco de dados são importantes para que a equipe de operação saiba onde deve executar a mudança. Mesmo não sendo de preenchimento obrigatório, os campos *Hostname*, *Instância* e *Owner* de Aplicação devem ser preenchidos para não haver dúvidas do local de atendimento da RDM.

O analista deve preencher também os campos comentário de implementação, número e descrição da *request*, para que o time de operação saiba qual requisição do CCS deve ser transportada para o ambiente produtivo.

Com o preenchimento dos campos citados, ou no mínimo os de preenchimento obrigatório, o analista de sistemas pode clicar em “Salvar”, momento em que o CRM Dynamics gera o identificador da mudança e manda um e-mail automático informando da criação da RDM para o usuário solicitante. Neste momento a situação da RDM é “Nova”.

A figura 14 ilustra as atividades realizadas automaticamente pelo CRM Dynamics, subprocesso do processo representado na figura 8.

Figura 14 - Procedimento automático do CRM ao criar a RDM.



Fonte: Elaborado pelo autor

Após o CRM Dynamics passar a RDM para situação “Nova”, automaticamente é gerada uma tarefa de aprovação e encaminha um e-mail para os usuários envolvidos informando da tarefa de aprovação pendente na RDM. O CRM Dynamics, também de forma automática, passa a RDM para a situação “Em aprovação”. Neste momento a RDM já começa a constar nos relatórios da Governança de TI e na fila de atendimento do grupo de suporte.

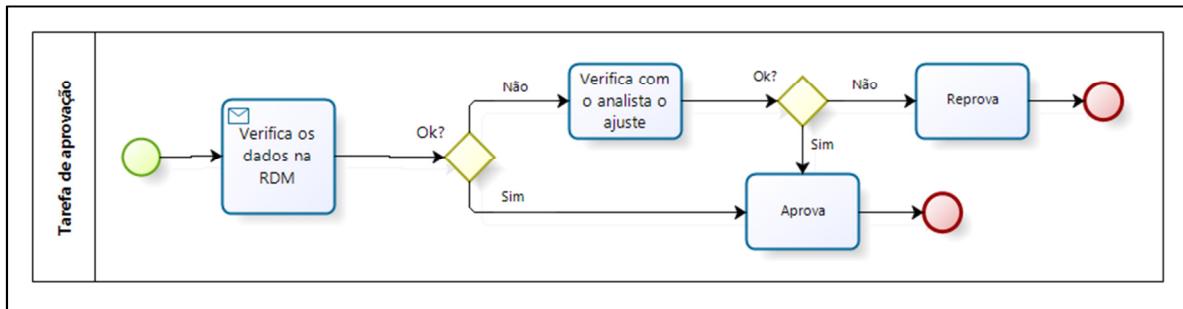
#### 4.3.2 Aprovação da RDM

Quando a tarefa de aprovação é criada, o CRM Dynamics já preenche com um responsável pela aprovação. O responsável pela aprovação inicial é algum usuário *default* definido para o assunto selecionado na RDM. Este usuário é alterado pelo analista de sistemas, sendo a tarefa de aprovação da RDM encaminhada a quem irá aprovar, sendo que este deverá ser comunicado via e-mail sobre a aprovação pendente.

A aprovação na CPFL obedece a orientações da ISACA (2011), que sugere que qualquer alteração deve fornecer provas de autorização e deve ter uma referência cruzada com o código fonte (número de requisição), devendo estar disponível para revisão.

A mudança deve ser aprovada por um responsável na TI, sendo que este deve constar na relação de aprovadores de mudanças controlada pela governança. A figura 15 ilustra os passos realizados no subprocesso Tarefa de Aprovação, presente na figura 8 que apresenta toda a RDM.

Figura 15 - Tarefa de Aprovação da RDM



Fonte: Elaborado pelo autor

A tarefa de aprovação da RDM pode ser respondida através do Portal de Serviços ou pelo próprio CRM. O responsável pela aprovação, antes de aprovar, deve verificar se a RDM tem os campos preenchidos com valores coerentes e se há vínculo com uma solicitação do usuário. Se ele não estiver de acordo, deve questionar o usuário a respeito. Sem retorno e/ou ajuste da RDM, deve reprová-la.

No caso da reprovação da RDM, ela entra em estado conclusivo, não podendo ser mais alterada. Neste momento o CRM Dynamics automaticamente encaminha para o usuário um e-mail informando que a RDM foi reprovada. A partir disto, a mudança não pode mais ser realizada, somente consta nos relatórios da Governança de TI.

Se o responsável aprovar a mudança, ela passa a constar na fila de atendimento da equipe responsável como “Em atendimento”. A equipe pode dar prioridade ao atendimento caso o analista de sistemas sinalize esta necessidade, ou esperar o momento da execução conforme a priorização interna da equipe.

#### 4.3.3 Execução da RDM

A execução de uma RDM é responsabilidade da equipe de operações da TI. Este procedimento segue a orientação da ISACA (2011), que diz que os programadores não devem ter acesso para modificar, gravar ou excluir dados de produção, sendo esta responsabilidade de um grupo que é independente da equipe de programação de computadores. O procedimento está de acordo também com as orientações da SOX na seção 2.6, que exige controle de acessos e privilégios aos usuários.

A mudança é executada conforme planejamento técnico e ao final da execução existe um plano de comunicação da execução da mudança. O responsável por atender a RDM relata o ocorrido no registro da mudança, e no caso de problemas, a mudança será cancelada ou não

atendida, dependendo do ocorrido, e as ações de correção ou reenvio devem ser encaminhadas.

A execução depende de uma análise prévia de impacto, para evitar problemas nas aplicações e evitando inconsistências e indisponibilidade nos sistemas. Sendo que todas as áreas devem seguir as normas e procedimentos estabelecidos para execução deste procedimento.

Os últimos campos na RDM são referentes à execução da RDM, ficando por conta da equipe de operação preencher estes campos, mostrando qual o resultado obtido, quando a RDM foi atendida, por quem e se foi com sucesso. O time de operação tem um papel fundamental nesta etapa do processo, já que somente eles têm permissão para executar alterações no ambiente produtivo.

A figura 16 apresenta estes campos da RDM. O campo anotações se trata de um local onde são inseridos comentários e arquivos pelos usuários, por exemplo, o plano de testes com homologação do usuário, não sendo este seu lugar obrigatório, mas que facilita o trabalho da Governança de TI no momento de procurar as evidências.

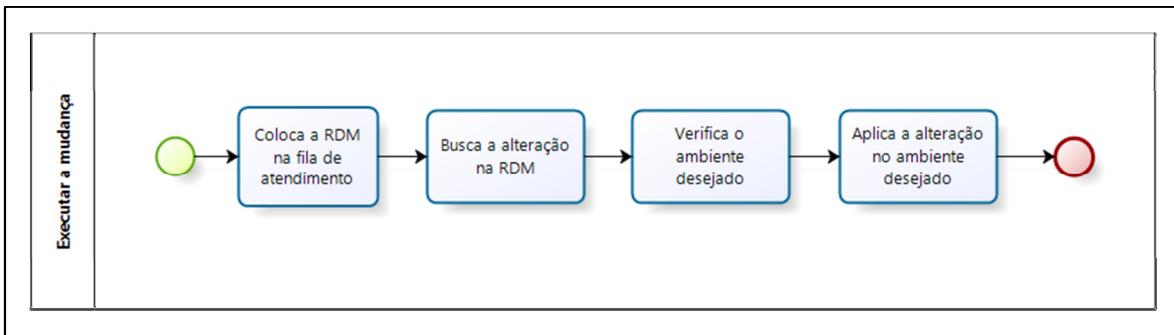
Figura 16 - Informações sobre a implementação da RDM e Anotações

Fonte: Microsoft Dynamics CRM (2011)

Para a execução da mudança, o analista de operação responsável por atender a RDM primeiramente inclui a mesma na sua relação de prioridades, baseado em procedimentos internos da equipe que não são auditados pela Lei SOX, portanto, não constam neste trabalho.

A figura 17 representa o subprocesso Executar mudança, presente na figura 8, representando o que é realizado na execução da RDM.

Figura 17 - Execução da RDM



Fonte: Elaborado pelo autor

Para executar a mudança, o analista de operação utiliza a solução passada pelo analista de sistemas, copia para a sua ferramenta de trabalho e então aplica a alteração em produção. Estas informações são incluídas pelo analista de sistemas nos respectivos campos da RDM.

No caso de falha na implantação da alteração, o plano de retorno é realizado pelo analista de operação e a mudança é passada para “Não atendida”, através da seleção da opção “Não” no questionamento “Implementado com sucesso?” na própria RDM e o CRM Dynamics comunica o não atendimento da RDM para os usuários envolvidos.

Com o preenchimento dos dados referentes à execução da mudança nos respectivos campos na RDM e sinalização da equipe de operação no CRM Dynamics para finalizar a mudança, ela é concluída. Uma RDM não pode ser reaberta, logo fica no CRM Dynamics somente para consultas posteriores, fazendo parte dos relatórios da Governança de TI sobre as mudanças realizadas no ambiente.

Caso a conclusão da RDM seja com sucesso, o CRM Dynamics automaticamente encaminha um e-mail para o proprietário da RDM e para o responsável pela aprovação informando que a RDM foi atendida. Este procedimento automático do CRM está de acordo com as orientações de revisões pós-implementação do COBIT (2007) no capítulo 3.

Com a sinalização por e-mail realizada pelo CRM Dynamics, o analista de sistemas está livre para testar se sua alteração atendeu o que foi solicitado pela área de negócio. Caso não atenda, uma nova RDM deve ser aberta e o ciclo começa novamente.

Quando do atendimento da RDM, o analista de operação preenche os campos com a data da implementação, usuário que realizou a implementação, se foi realizada com sucesso e o resultado da implementação.

A partir desse momento a RDM é automaticamente passada para o estado conclusivo “Atendida” e o CRM Dynamics não permite mais alterações, então ela passa somente a constar nos relatórios da governança de TI.

Após o preenchimento de todos os campos, a RDM pode ser finalizada. O analista responsável deve encerrar a RDM através do próprio CRM Dynamics, assim a ferramenta fará os processos necessários para comunicar área de negócio, analista de sistemas e aprovador da RDM.

#### **4.3.4 Cancelamento da RDM**

Durante o ciclo de vida da RDM, qualquer um dos usuários envolvidos pode acessar o CRM Dynamics, marcar “Sim” na opção “Cancela RDM”, preencher o campo específico que o CRM Dynamics abre para a justificativa e salvar a mudança. Esta ação passará a RDM para um estado conclusivo, que não pode ser alterado.

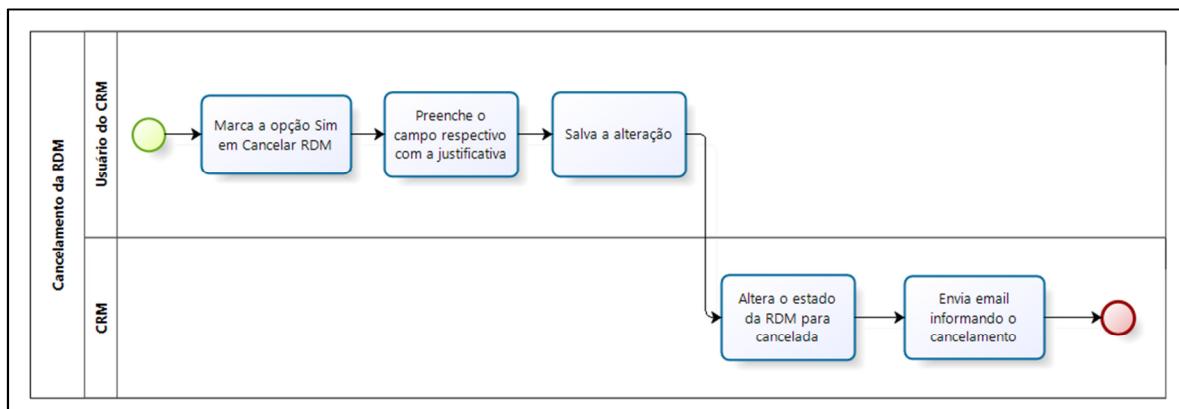
Esta alteração de estado da RDM fica registrada junto com as demais modificações realizadas na RDM pelos usuários ou pelo próprio CRM Dynamics quando este faz alterações automáticas pelo fluxo de trabalho utilizado.

No cancelamento da RDM, o CRM Dynamics automaticamente encaminha um e-mail para o proprietário da RDM informando que a RDM foi cancelada e o motivo pelo qual foi cancelada, preenchido pelo responsável em campo específico da RDM.

Os e-mails, que são enviados pelo próprio CRM Dynamics, são automaticamente salvos na guia Atividades Fechadas, na RDM, não havendo possibilidade de alteração destes registros. Conforme a ISACA (2011), este histórico com todas as atividades da RDM é um dos pontos que permite o rastreamento de informações na auditoria de SI.

A figura 18 ilustra o processo de cancelamento, que não consta na figura 8 por ser uma situação esporádica, não havendo uma condição específica em que este procedimento ocorra.

Figura 18 - Processo de cancelamento da RDM



Fonte: Elaborado pelo autor

#### 4.4 ANÁLISE SUMARIZADA DO PROCESSO ATUAL

No caso do grupo CPFL, os riscos no processo de auditoria já estão mapeados, porém, estes dados são sigilosos, não podendo ser expostos neste trabalho. Somente os controles de auditoria, criados a partir da análise de riscos, podem ser utilizados.

Os controles de auditoria definidos estão de acordo com as melhores práticas de governança de TI. Tais controles atuam com os objetivos de monitoramento, prevenção e conscientização, sendo classificados como preventivos e detectivos.

A tabela 2 apresenta os controles de auditoria da CPFL referentes a gestão de mudanças, a evidência utilizada para sanar o respectivo ponto de auditoria e referenciais teóricos que fundamentam esta evidência.

Tabela 2 - Controles identificados

(continua)

Controle	Evidência	Referencial Teórico
As mudanças devem ser aprovadas por um responsável pelas aprovações conforme a lista da governança	Informações da RDM (colunas Aprovador 1 e Data de Aprovação 1)	ISACA (2011), ITIL (2007), Imoniana (2008)
Realização de testes para verificação do resultado obtido com a RDM.	E-mail do CRM Dynamics (enviado aos analistas de sistemas)	CobiT (2007)
Restrição de acesso para que somente a equipe de operação possa realizar as mudanças em produção	Implementadores RDMs	ISACA (2011), SOX (2002), ITIL (2007)
Mudanças originadas a partir de uma solicitação a área de negócio	Informações da RDM (coluna Origem da RDM)	ITIL (2007)

(conclusão)

Controle	Evidência	Referencial Teórico
A empresa deve ter um procedimento padrão para as mudanças no ambiente de TI	Metodologia de Manutenção de Sistemas	SOX (2002), Gil (1999), ISACA (2011), Imoniana (2008)
Campos preenchidos na RDM com todas as informações necessárias para atendimento.	Informações da RDM	ISACA (2011)
Cada mudança deve estar registrada na ferramenta CRM Dynamics e constar nos relatórios da governança	Controles da Governança	ISACA (2011), SOX (2002)
A governança deve ter controle sobre as mudanças criadas no CRM Dynamics	Controles da Governança	ISACA (2011), SOX (2002)
Um plano de teste é elaborado e os testes são realizados e comprovados para todas as mudanças nos sistemas	Homologação (email do usuário ou atividade no CRM Dynamics)	ISACA (2011), SOX (2002), Imoniana (2008), CobiT (2007)
Os sistemas estão adequadamente configurados para registrar as alterações realizadas por usuários	Histórico de Auditoria	ISACA (2011), Lyra (2008),

Fonte: Elaborado pelo autor

Os pontos de controle presentes na tabela 2 já são solucionados no atual processo existente na CPFL. Junto a estes, o processo apresentado neste capítulo, apresenta procedimentos que correspondem ao referencial teórico apresentado neste trabalho.

A tabela 3 apresenta características do processo atual, os pontos positivos encontrados referenciais teóricos que apoiam estes pontos positivos.

Tabela 3 - Pontos positivos do processo atual

(continua)

Característica	Ponto positivo encontrado	Referencial Teórico
Metodologia de Manutenção de Sistemas	Metodologia padrão estabelecida e publicada para gerenciamento de mudanças em SI	ISACA (2011), Gil (1999), SOX (2002), Imoniana (2008)
Formulário da RDM	Formulário padrão para requisição da mudança em um sistema de gerenciamento de mudanças.	ISACA (2011)
Aprovação da RDM	Fluxo de aprovação automático no sistema de gerenciamento de mudanças, não havendo andamento da RDM sem a aprovação.	ITIL (2007), ISACA (2011), Imoniana (2008)
Análise de impacto	Campo para descrição do impacto da alteração presente no formulário da RDM.	ITIL (2007)
Análise de risco	Campo para descrição de risco da alteração presente no formulário da RDM.	ABNT (2008), ITIL (2007)

(conclusão)

Característica	Ponto positivo encontrado	Referencial Teórico
Plano de retorno	Campo para descrição do plano de retorno presente no formulário da RDM.	ISACA (2011), ITIL (2007), CobiT (2007)
Histórico de Logs	Automatização de logs permitindo a rastreabilidade de todas as alterações realizadas em uma RDM.	ISACA (2011)
Homologação	Processo de aprovação do usuário de negócio das alterações realizadas antes da passagem para produção.	ISACA (2011), SOX (2002), Imoniana (2008), CobiT (2007)
Execução pela Operação	Restrição de acesso que permite que somente a equipe de Operação possa executar as mudanças no ambiente de produção.	ISACA (2011)
Restrição de Acessos	Os acessos dos usuários são restritos às suas funções.	ISACA (2011), SOX (2002), ITIL (2007)

Fonte: Elaborado pelo autor

#### 4.5 PROBLEMAS DO PROCESSO ATUAL

Para realização de manutenção do sistema CCS, a equipe de TI do Grupo CPFL utiliza uma metodologia que não deixa claro onde e como cada uma das evidências deve ser criada e registrada para uma posterior coleta de evidências em auditorias realizadas para manter a certificação da SOX.

Devido à ausência de um processo que defina o registro das evidências, quando ocorrem auditorias, os analistas de sistemas se deparam com questionamentos da Governança de TI sobre evidências faltantes no CRM Dynamics. A ausência destas evidências é registrada nos laudos da equipe de auditoria.

As auditorias externas são as mais detalhistas, sendo feitas por empresas contratadas pelo grupo para realização das avaliações necessárias em todos os processos da empresa e assim garantir as suas certificações.

Nestas avaliações, são verificadas as RDMs atendidas, sendo que cada uma delas deve ter as evidências necessárias conforme orientado na MMS, utilizada pelo departamento de TI do grupo.

Nas auditorias, a equipe de Governança de TI encaminha uma relação com as RDMs do período desejado para a auditoria externa, que seleciona aleatoriamente entre 20 e 25 RDMs da relação para serem auditadas. Para estas, a equipe de Governança de TI busca no CRM Dynamics as evidências de cada uma.

Com a migração do sistema comercial CCS para a RGE, e o novo processo disponibilizado para as equipes de atendimento na TI, o objetivo é que fique mais difícil haver falhas quanto ao registro de evidências para validações da SOX nas RDMs. Na utilização tanto da MMSS na RGE, como da MMS nas outras empresas do Grupo CPFL, com frequência, durante as auditorias, faltam evidências necessárias nas mudanças.

Este problema pode ocorrer por vários motivos, entre eles:

- O time de operação é pequeno e o número de mudanças realizadas diariamente é grande, possibilitando falhas em alguma etapa do procedimento;
- Quando dois ou mais membros da equipe de operação se envolvem no atendimento de uma mesma RDM, devido a troca de turnos, podendo haver falha na comunicação entre os operadores;
- As metodologias utilizadas pelas equipes são pouco específicas sobre o registro de cada evidência que deve ser registrada neste procedimento;
- O grande número de mudanças realizadas pela equipe de manutenção de sistemas, onde o analista pode accidentalmente não anexar todas as evidências, já que o procedimento é manual.

Quando a equipe de governança de TI encontrar uma falha no registro das evidências, o analista de sistemas responsável pela mudança (solicitante) é contatado para providenciar a evidência faltante e anexar na RDM pelo CRM Dynamics. Quando esta situação ocorre na auditoria externa, isso é considerado um ponto de auditoria, pois não segue o descrito no controle.

A tabela 4 mostra, de forma sumarizada, características do processo e falhas encontradas.

Tabela 4 - Problemas no processo atual

(continua)

<b>Característica</b>	<b>Problema encontrado</b>
Local das evidências	As evidências não tem padrão de local e estrutura para arquivamento
Identificação das evidências	Não há padrão da nomenclatura das evidências coletadas
Status das evidências da RDM	Não há um documento formal com um parecer da equipe de Governança de TI sobre evidências coletadas.

(continua)

Característica	Problema encontrado
Backup das evidências	Não há um arquivamento de backup para posterior consulta nas evidências enviadas para os auditores.
Controle das RDMs	A Governança de TI não tem relatórios de todas as RDMs referentes aos sistemas comerciais, mas somente das RDMs atendidas.

Fonte: Elaborado pelo autor

## 4.6 CONSIDERAÇÕES FINAIS

Este capítulo apresentou o ambiente do sistema comercial utilizado pelo Grupo CPFL, o sistema CCS, a metodologia de manutenção de sistemas utilizada, o procedimento da RDM, as ações realizadas neste procedimento, uma análise sumarizada do processo descrito quanto ao referencial no qual este trabalho está baseado e os problemas encontrados neste processo.

O procedimento realizado pelos analistas de sistemas, com atuação da área de negócio, deve sempre obedecer ao que foi alinhado com a Governança de TI do Grupo CPFL. Mesmo quando alguma destas regras não estiver na última versão publicada da metodologia no GED CPFL.

Atualmente, quando do período da auditoria, a Governança de TI avalia as RDMs no CRM Dynamics e, caso encontre alguma inconformidade, questiona o analista de sistemas solicitante da RDM. Nesta avaliação pode ser utilizado o Histórico de Auditoria das RDMs para auxiliar na busca de uma inconformidade.

Para controle das RDMs por parte da equipe de Governança de TI, o COBIT (2007) orienta na seção 3.2 sobre a utilização de relatórios de mudanças para acompanhar o que foi rejeitado ou atendido, podendo acompanhar cada RDM e validar as evidências anexadas.

Como não há no momento um processo que diga onde e como uma evidência deve ser registrada para uma posterior coleta, é difícil para a governança de TI garantir que encontrará as evidências para uma auditoria da SOX.

Devido ao número elevado de mudanças realizadas por cada analista e atendidas pela equipe de operação, em alguns casos, as RDMs não têm as evidências necessárias, já que o processo não é claro. No capítulo seguinte é a presentada a solução proposta para os problemas encontrados no processo atual.

## 5 PROPOSTA DE SOLUÇÃO

A solução proposta para o problema encontrado é o desenvolvimento de um processo que apresente exatamente em que momento e como deve ser criada cada uma das evidências SOX, complementando a MMS. É importante lembrar que este trabalho não interfere nas atividades realizadas pelos auditores externos, somente define a forma como devem ser registradas as evidências que serão enviadas para a equipe de auditoria.

Este capítulo tem como objetivo apresentar o processo proposto, criado com a intenção de melhorar o processo existente e diminuir os problemas encontrados nas auditorias de sistemas comerciais, inclusive o recurso de Histórico de Auditoria, importante no processo.

Este capítulo apresenta também as diferenças existentes entre o processo atual e o proposto, e como os usuários deverão ser orientados a respeito.

### 5.1 NOVO PROCESSO

Considerando o contexto descrito no capítulo 4 deste trabalho, sobre como é realizado o procedimento de passagens para produção, o processo proposto apresenta um novo cenário, onde um processo mais eficaz fica disponível a todos os envolvidos, auxiliando nas suas atividades.

Com este novo procedimento complementando a MMS, quando cada analista de sistemas for abrir uma RDM, poderá seguir os passos descritos, sabendo como trabalhar as evidências, minimizando impactos negativos nas auditorias.

O trabalho da equipe de Governança de TI fica mais fácil havendo um padrão para localizar as evidências e sabendo que as equipes de atendimento estão devidamente orientadas sobre como proceder.

Para disponibilizar o processo a todos os envolvidos, o material proposto pode ser incluído na documentação da própria metodologia de manutenção de sistemas ou ainda ser publicado no GED CPFL, ficando a cargo da Governança de TI definir a melhor forma de fazer a publicação.

Estas ações irão diminuir significativamente o número de RDMs encontradas durante as auditorias sem as evidências necessárias para atender os requisitos legais pertinentes a Lei SOX.

O novo processo respeita conceitos da ITIL, COBIT, ABNT e ISACA, apresentados no referencial teórico deste trabalho, com o objetivo de facilitar o trabalho dos analistas de sistemas, de operação e de governança de TI.

São considerados os referenciais bibliográficos presentes no capítulo 2 sobre auditoria. Os levantamentos realizados sobre controles de auditoria, técnicas de coleta de evidências e impactos da Lei SOX são pilares do processo elaborado.

Para a realização do registro das evidências para as auditorias, o analista responsável deverá utilizar o diagrama proposto como guia, sabendo quais são e onde devem ficar registradas as evidências necessárias em uma RDM.

O novo processo apresenta o Histórico de Auditoria como um recurso para validar as evidências que são informações preenchidas no formulário da RDM. Este recurso já existe no CRM Dynamics no Grupo CPFL, porém não é utilizado para fins de auditoria.

A subseção 5.1.1 apresenta o Histórico de Auditoria, uma ferramenta importante para verificar a veracidade das informações inseridas em uma RDM, a subseção 5.1.2 contém premissas assumidas para criação da RDM, e as subseções 5.1.3 e 5.1.4 apresentam a geração das evidências durante o ciclo de vida da RDM. A subseção 5.1.5 apresenta controles adicionais que foram criados neste trabalho para auxiliar a governança de TI na identificação de problemas com as informações inseridas nas RDMS.

### **5.1.1 Histórico de Auditoria**

Conforme a ISACA (2011), o sistema de gerenciamento de mudanças deve permitir o rastreamento de todas as informações da RDM, tais como programador atribuído, alterações feitas e data em que foi fechada.

Nesta mesma linha, Lyra (2008) afirma que é importante que todos os sistemas possuam registro das atividades realizadas pelos seus usuários, que devem registrar informações como data e hora, tipo de atividade e valor antigo e valor novo, para que seja possível a auditoria em caso de violação da integridade da informação.

Para tanto, a RDM no CRM Dynamics possui um recurso chamado Histórico de Auditoria. Neste histórico são registrados logs de todas as alterações realizadas em qualquer campo da RDM. Tais dados são: Data da alteração, Alterado por, Evento, Campo Alterado, Valor Antigo e Novo Valor.

Este histórico, que é gerado automaticamente pelo CRM Dynamics, pode ser consultado na própria RDM, mas não é possível a realização de alterações nestes dados,

reforçando o princípio de auditabilidade proposto por Lyra (2008).

A figura 19 apresenta um exemplo de Histórico de Auditoria de uma RDM.

Figura 19 - Exemplo de Histórico de Auditoria

Data da Alteração	Alterado por	Evento	Campo Alterado	Valor Antigo	Novo Valor
10/02/2015 09:33	Adm Prd Crm	Desativar	Data de Modificação	10/02/2015 09:33	10/02/2015 09:33
			Modificado Por	Luiz Fernando Portella (s...)	Adm Prd Crm
			Modificado por (Deleg...)		
			Razão do Status	Em Atendimento	Atendida
			Status	Ativo(a)	Inativo(a)
10/02/2015 09:33	Luiz Fernando Portel...	Atualizar	Comentário da Imple...	A ser preenchido.	número de regs confere
			Data de Modificação	09/02/2015 18:21	10/02/2015 09:33
			Data Real de Impleme...	09/02/2015	10/02/2015

Fonte: Microsoft Dynamics CRM (2011)

O campo “Alterado por” registra o nome do usuário que está autenticado no computador no momento da alteração. A autenticação dos usuários ocorre no domínio da CPFL, onde há uma política de acesso aplicada a todos os colaboradores, conforme orientado na seção 2.8. Essa política exige, por exemplo, que a senha do usuário siga os critérios abaixo:

- Tamanho mínimo de senha: 8 caracteres;
- Tempo de expiração de senha: 60 dias;
- Bloqueio de usuário por tentativas inválidas: 5 tentativas;
- Restrição de últimas senhas utilizadas: 4 senhas;
- Complexidade de senhas: habilitado.

A autenticação dos usuários e os logs presentes no Histórico de Auditoria da RDM garantem a auditabilidade e acuracidade, dois objetivos da auditoria apresentados por Lyra (2008). Estes registros ajudam a garantir a integridade, validade, verificabilidade, consistência e a confiabilidade dos dados, conforme a ISACA (2011).

Este recurso deve ser utilizado pela equipe de governança de TI nos casos em que é necessário analisar detalhadamente quais alterações foram realizadas pelos usuários para se ter certeza se o procedimento foi realizado corretamente.

### 5.1.2 Premissas para criação da RDM

A primeira premissa deste processo é a vigência de uma metodologia que oriente os usuários sobre a forma como deve ocorrer a manutenção de sistemas. Para tanto, a CPFL tem a MMS, descrita na seção 4.2, publicada no GED CPFL.

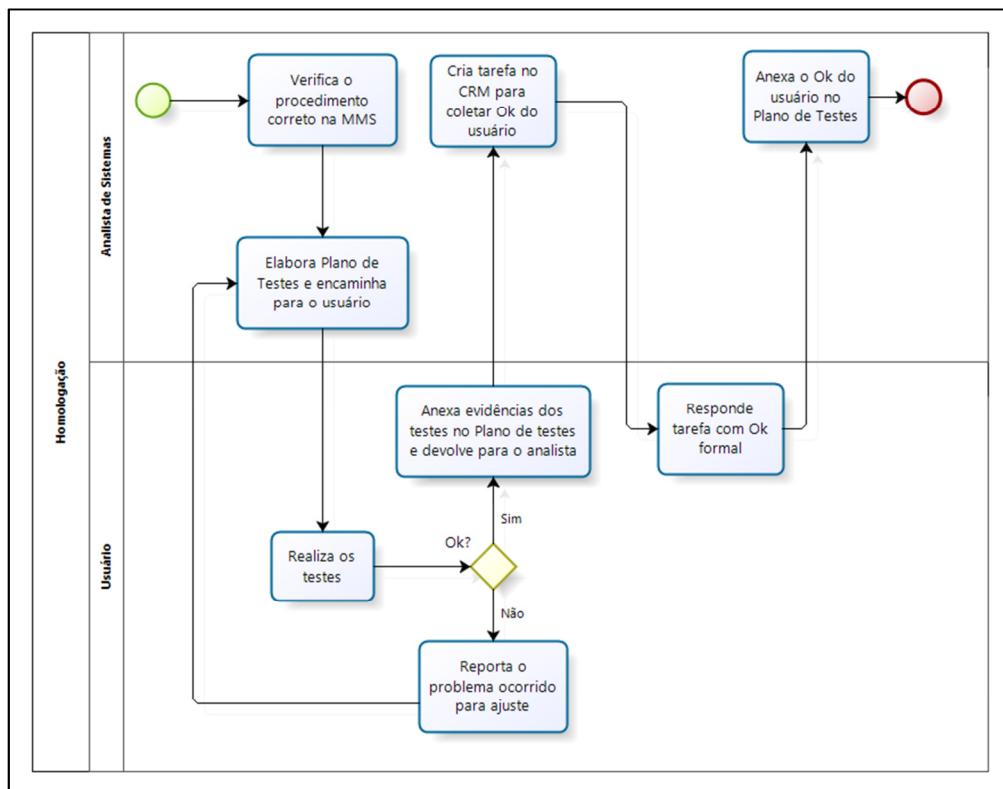
A segunda premissa é a homologação. Para que uma RDM seja criada, parte-se do princípio que a alteração que será transportada para o ambiente de produção já foi previamente homologada pelo usuário solicitante.

A homologação deve ocorrer através de um documento de plano de testes padrão do grupo CPFL, onde estão descritos os passos que devem ser seguidos pelo usuário, nos cenários de testes desenhados pelo analista de sistemas, para determinar se a solução está conforme solicitado. A utilização de um plano de testes é uma orientação presente no referencial teórico deste trabalho. O documento padrão do Grupo, disponível no Anexo G, inclui as seguintes informações:

- Identificação da solicitação do usuário;
- Informações sobre os envolvidos no atendimento;
- Impactos da mudança;
- Orientações sobre a realização dos testes;
- Cenários de Teste;
- Capturas de tela dos testes realizados;
- Questionário de aceitação;
- Capturas de tela com a aceitação.

A captura de tela com a aceitação do usuário da homologação deve ser a partir de uma tarefa criada na solicitação do usuário no próprio CRM Dynamics. Após o recebimento do plano de testes com as evidências de testes e retorno positivo do usuário, o analista de sistemas deve abrir esta tarefa no CRM Dynamics e solicitar aprovação do usuário, que ficará registrada na ferramenta. Nesse caso, a captura de tela é algo manual, mas a solicitação de aprovação é automatizada e a resposta do usuário fica armazenada diretamente no CRM Dynamics, sem possibilidade de sofrer alterações indevidas. Além disso, o registro ficará disponível para consultas posteriores caso necessário. A figura 20 apresenta o processo descrito.

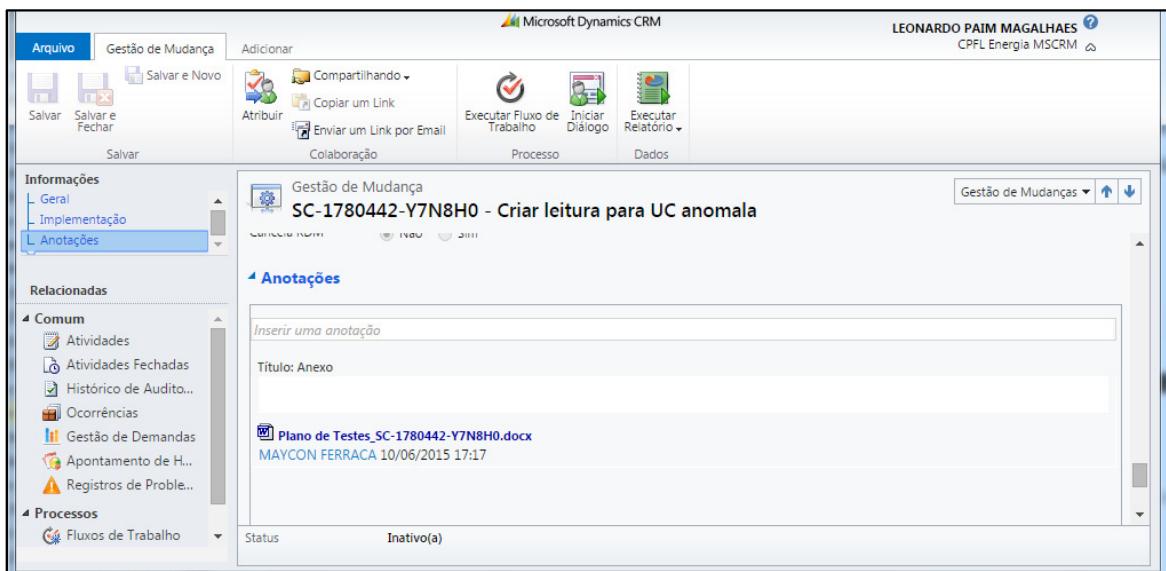
Figura 20 - Premissa para criação da RDM



Fonte: Elaborado pelo autor

O plano de testes deve ser anexado na aba Anotações da RDM pelo analista de sistemas que criar a RDM no CRM Dynamics. Caso este documento não esteja anexado na RDM, ela não será aprovada na próxima etapa. A figura 21 mostra um exemplo de como deve ficar o plano de testes nas anotações da RDM.

Figura 21 - Plano de Testes nas Anotações da RDM



Fonte: Microsoft Dynamics CRM (2011)

### 5.1.3 Criação/Aprovação da RDM

As diferenças entre esta seção e a descrição das seções 4.3.1 e 4.3.2 estão no preenchimento correto dos campos que são auditados e na forma como deve ocorrer a aprovação da mudança. Estes dados estarão presentes no Histórico de Auditoria tanto da própria RDM quanto da tarefa de aprovação da mesma.

Para a criação da RDM, conforme já descrito, o CRM Dynamics tem um formulário padrão, conforme orientado no referencial teórico deste trabalho. Todos os valores preenchidos ficam salvos no Histórico de Auditoria da RDM.

Nesta etapa, é necessário que o usuário preencha os campos Origem da RDM, Riscos Associados, Descrição do Impacto e Plano de Retorno. Estes são os campos solicitados na SOX e nas normas estudadas.

Estes campos são os que estarão nos relatórios de controle das RDMs, então, é importante que as informações estejam corretas. O analista não deve preencher eles com informações aleatórias (Ex: “xxxxxxxxxx”).

No campo “Mudança” é preenchido o título, onde o analista de sistemas deve preencher primeiramente com número da solicitação que originou a mudança, e uma referência ao que será realizado (Ex: “DEM-0012345 – Ajuste relatório contábil”), facilitando a rastreabilidade da mudança posteriormente.

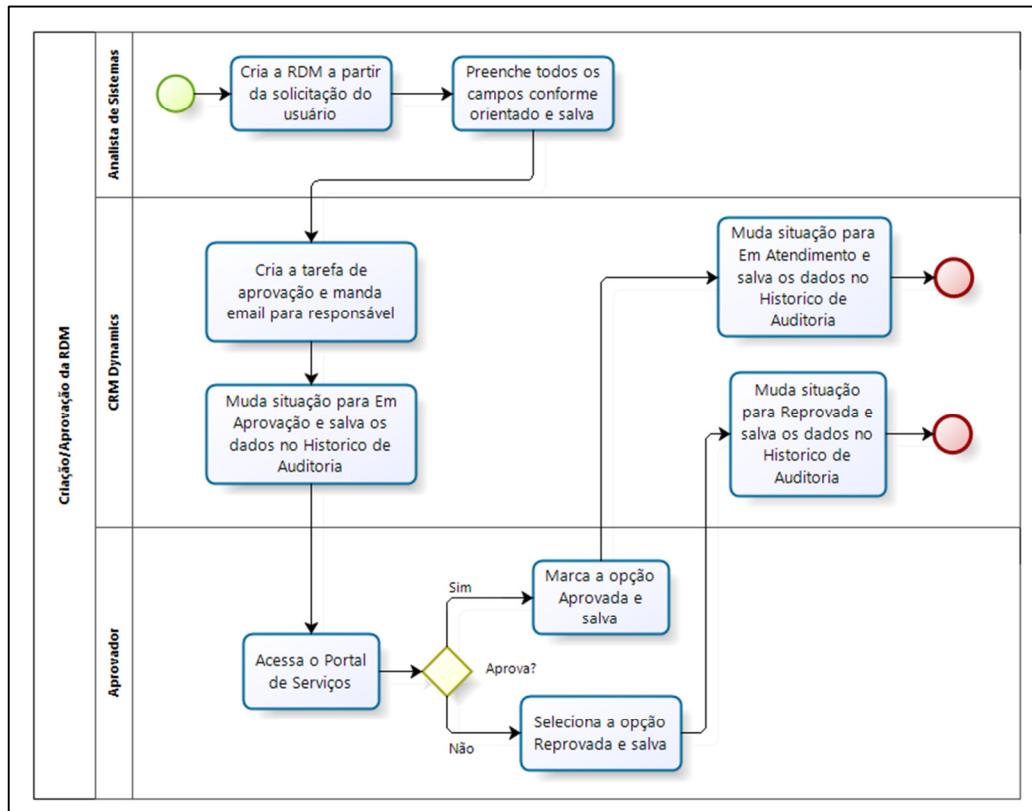
Os campos “Demanda Relacionada”, “Ocorrência” e “Registro de Problemas” são os campos onde o analista de sistemas deve preencher com o número identificador da solicitação que está atendendo da área de negócio, criando um vínculo entre a RDM e a solicitação do usuário, permitindo a rastreabilidade da RDM.

Após o preenchimento de todos os campos da RDM, ao salvá-la, o CRM automaticamente envia o email de aprovação para o responsável pela aprovação. Este responsável pela aprovação é o responsável pelo assunto atribuído à RDM, sendo um dos membros na TI previamente autorizado pela governança de TI para esta aprovação.

O responsável pela aprovação da tarefa não deve ser alterado sem prévia autorização da gerência e da governança de TI. Caso ocorra, este registro deve ser anexado na tarefa de aprovação.

O responsável pela aprovação deve verificar se a RDM atende aos quesitos estipulados pela sua gerência. A tarefa de aprovação deve ser respondida através do Portal de Serviços, para que os logs fiquem salvos da maneira correta no Histórico de Auditoria da própria tarefa no CRM Dynamics. A figura 22 mostra como fica este processo.

Figura 22 - Criação e Aprovação da RDM



Fonte: Elaborado pelo autor

A RDM pode não ser aprovada pela TI, então seu estado conclusivo ficará como Reprovada. Caso isso ocorra, ela não pode mais sofrer alterações e somente constará no respectivo relatório dos controles da governança de TI.

#### 5.1.4 Conclusão da RDM

As diferenças entre os passos descritos nesta seção e os que estão na seção 4.3.3, referente à conclusão da RDM, não estão nos procedimentos realizados, mas no resultado destes. A utilização do Histórico de Auditoria, apresentado na subseção 5.1.1, permite a validação das informações inseridas nesta etapa, podendo-se encontrar, por exemplo, casos onde um usuário que não tem permissão para execução de uma RDM, fez o encerramento da mesma. Além disso, o resultado desta etapa da mudança é ponto fundamental para os relatórios que serão apresentados na subseção 5.1.5.

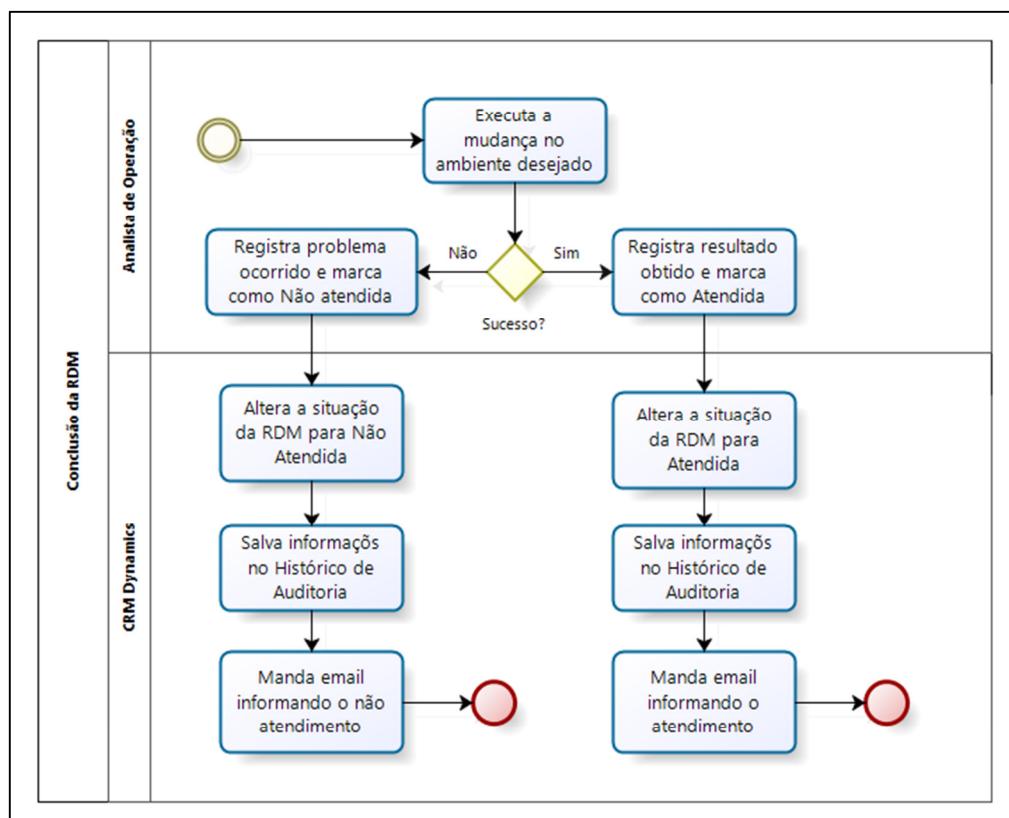
Após o transporte da RDM para o ambiente de produção, o analista de operação deverá preencher os campos referentes a implementação da mesma e concluir-la. Todos os

campos preenchidos nesta etapa ficam salvos no Histórico de Auditoria da RDM.

O campo “Implementado Por” deve ser preenchido com o nome do analista que está atendendo a RDM. Este usuário deve ter os privilégios necessários para esta operação, sendo previamente autorizado pela gerência e governança de TI para tal atividade.

A RDM pode não ser atendida com sucesso. Neste caso, ela poderá ser concluída como Não Atendida. A figura 23 mostra este processo.

Figura 23 - Conclusão da RDM



Fonte: Elaborado pelo autor

Para facilitar a pesquisa pelos usuários que implementaram RDMs em determinado período, foi criado e disponibilizado o Relatório Auditoria SOX - Implementadores RDMs (exemplo no Anexo F).

O CRM encaminha um email automaticamente no momento da conclusão da RDM para o analista solicitante verificar se a alteração foi aplicada conforme previsto, ou para informar o solicitante que a RDM não foi atendida.

Caso a conclusão da RDM seja por cancelamento, o que pode acontecer em qualquer momento após a sua criação, o usuário deve anexar nas anotações da RDM a formalização do cancelamento da RDM, para que este possa ser consultado posteriormente.

### 5.1.5 Controle de RDMs

Para um controle das RDMs após a sua conclusão, conforme definido pela SOX, apresentada na seção 2.6, devem haver relatórios que apresentem as RDMS referentes a sistemas comerciais. Não há determinação na lei de quantos relatórios sejam e de como eles devem ser, desde que contemplam as mudanças conforme os critérios de auditoria.

Além de atender a SOX, ter relatórios para controlar todas as mudanças geradas também é uma das orientações presentes no CobiT (2007) sobre a implementação de SI, conforme seção 3.2.

Para contemplar todas as RDMs, foram criados novos relatórios para controle de mudanças pela governança de TI, disponibilizados na Localização Avançada do CRM Dynamics. Segue o nome de cada um e as colunas que cada um possui:

- Relatório para Auditoria SOX – RDM Individual: Id da mudança, Origem da RDM, Riscos Associados, Descrição do Impacto, Plano de Retorno, Aprovador 1, Data de Aprovação;
- Relatório para Auditoria SOX – Canceladas: Id da mudança, Grupo de Suporte, Data de Criação, Razão do Status, Motivo do Cancelamento, Origem da RDM, Aprovador 1, Data da Aprovação, Descrição do Impacto, Riscos associados, Plano de Retorno;
- Relatório para Auditoria SOX – Não atendidas: Id da mudança, Grupo de Suporte, Data de Criação, Razão do Status, Origem da RDM, Aprovador 1, Data da Aprovação, Comentário de Implementação, Descrição do Impacto, Riscos Associados, Plano de Retorno;
- Relatório para Auditoria SOX – Atendidas: Id da mudança, Grupo de Suporte, Data de Criação, Razão do Status, Origem da RDM, Aprovador 1, Data de Aprovação, Comentário de Implementação, Data Real de Implementação, Implementado por, Descrição do Impacto, Riscos Associados, Plano de Retorno;
- Relatório para Auditoria SOX – Reprovadas: Id da Mudança, Grupo de Suporte, Data de Criação, Razão do Status, Origem da RDM, Aprovador 1, Data Aprovação, Descrição do Impacto, Riscos Associados, Plano de Retorno;
- Relatório para Auditoria SOX – Geral: Id da Mudança, Grupo de Suporte, Data de Criação, Razão do Status, Origem da RDM, Aprovador 1, Data de Aprovação, Descrição do Impacto, Riscos Associados, Comentário da

Implementação, Data Real de Implementação, Implementado por, Motivo do Cancelamento, Plano de Retorno.

Os relatórios foram construídos utilizando campos presentes na RDM. Para extração destes relatórios, o usuário terá somente que alterar as datas de criação nas exibições salvas para o período que estiver sendo auditado.

A figura 24 mostra a tela de elaboração do relatório de RDMs Não Atendidas como exemplo, e os Anexos A, B, C, D e E, mostram exemplos dos relatórios criados, um para cada estado conclusivo das RDMs. O anexo G mostra o exemplo de uma pesquisa individual a uma determinada RDM.

Figura 24 - Detalhes dos relatórios SOX

The screenshot shows the Microsoft Dynamics CRM interface for report creation. The top navigation bar includes 'Arquivo', 'Localização Avançada', 'Salvar como', 'Agrupar E', 'Agrupar OU', 'Consultar', 'Depurar', and 'Baixar Buscar XML'. The main area displays a search form for 'Gestão de Mudanças' with the query 'Relatório para Auditoria SOX - Não atendidas'. The search criteria are:

- Status: Iqual a Inativo(a)
- Razão do Status: Iqual a Não Atendida
- OU: (multiple entries under 'OU' dropdown)
- Data de Criação: Em ou Depois de 01/01/2014
- Data de Criação: Em ou Antes de 31/05/2015
- Assunto: (multiple entries under 'Assunto' dropdown)

The 'Assunto' dropdown contains the following items:

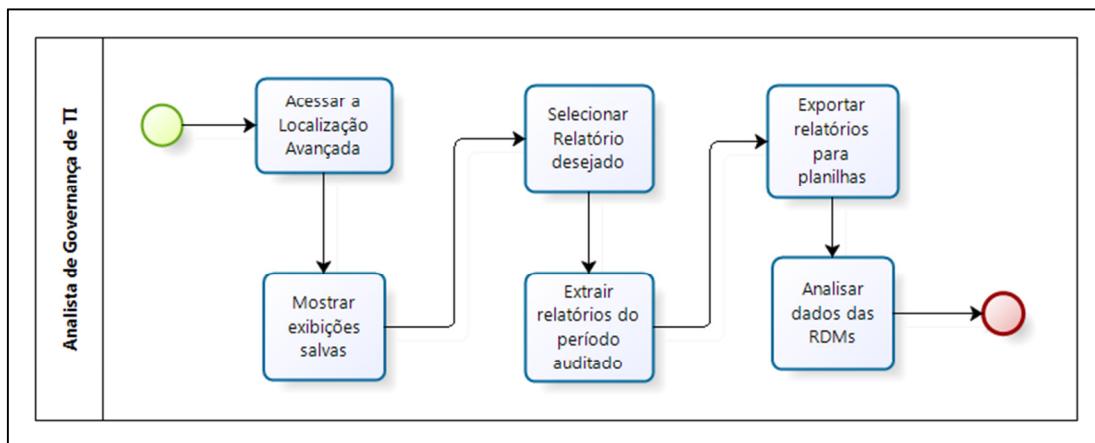
- SIS - SAP/CCS - ABAP/Java
- SIS - SAP/CCS - ACC
- SIS - SAP/CCS - Basis
- SIS - SAP/CCS - Cadeia Batch
- SIS - SAP/CCS - EDM
- SIS - SAP/CCS - FAT
- SIS - SAP/CCS - GAT/GLE
- SIS - SAP/CCS - IGE (BW)
- SIS - SAP/CCS - Mobile
- SIS - SAP/CCS - PEC
- SIS - SAP/CCS - SML A/B
- SIS - SAP/CCS - TAC (CRM 5...)
- SIS - SAP/CCS - WF
- SIS - SAP/CCS - WF - Tabela...

Fonte: Microsoft Dynamics CRM (2011)

Os relatórios disponíveis devem conter todas as RDMs referentes ao período auditado.

A ausência de alguma RDM que se enquadre nos parâmetros estipulados pela equipe de auditoria qualifica uma falha no controle interno utilizado. Os relatórios podem ser acessados no CRM Dynamics pelo analista e exportados para planilhas. A figura 24 mostra a extração dos relatórios.

Figura 25 - Controle de RDMs



Fonte: Microsoft Dynamics CRM (2011)

As primeiras colunas dos relatórios são utilizadas para identificação da RDM, da mesma forma que em outros relatórios já existentes na empresa. Mas, para os controles da governança, em concordância com as normas estudadas, os relatórios apresentam o vínculo com a solicitação do usuário, aprovação, quem atendeu a RDM e a descrição de seu impacto e risco, atendendo a pontos de controle apresentados neste trabalho.

## 5.2 DIFERENÇAS ENTRE OS PROCESSOS

Para deixar mais clara a contribuição deste trabalho, foi realizado um levantamento das diferenças encontradas entre o processo atual e o proposto. Este levantamento foi realizado durante o desenho do processo, onde ficaram claras as diferenças entre os dois cenários.

Para o analista de sistemas, a principal diferença é ter um referencial apontando onde a evidência deve ser gerada, tendo locais específicos para armazenar cada uma das evidências. No processo atual, apesar do fluxo de trabalho e restrições do CRM Dynamics, as evidências muitas vezes ficavam distribuídas na RDM ou até mesmo em outros locais do CRM Dynamics. Com um padrão de locais para a busca das evidências, o analista de governança de

TI responsável por coletar as evidências sabe exatamente onde procurar as evidências, facilitando o procedimento.

No processo proposto as evidências são diferentes. O processo atual se baseia basicamente em capturas de tela extraídas de diferentes locais. No novo processo, as evidências têm origem automatizada, como relatórios extraídos do próprio CRM Dynamics e fontes que dificultam alguma forma de manipulação.

A tarefa de aprovação, que no processo atual tem seu responsável alterado frequentemente, deverá ser aprovada pelo responsável pelo assunto cadastrado no CRM Dynamics, senão, a troca deverá ser justificada e aprovada previamente. Além disso, no processo atual, ela deve ser respondida através do Portal de Serviços, não mais pelo CRM, para que fiquem no CRM Dynamics os devidos registros.

A homologação, no processo proposto, passa a ser registrada no próprio CRM Dynamics, através de tarefas criadas a partir da solicitação do usuário, vinculada a RDM. Diferente dos e-mails, utilizados até então, este formulário ficará disponível para consulta de todos os envolvidos no procedimento. O plano de testes com o aceite do usuário deve estar sempre anexado na RDM, na aba Anotações.

O vínculo de uma RDM com a solicitação do usuário é feito tanto no título, que facilita a rastreabilidade em consultas no CRM Dynamics, quanto nos campos designados para esta função, que permitem que pela Localização Avançada, se identifique a partir da RDM qual Ocorrência, Demanda ou Problema a originou.

Para a governança de TI, no momento da auditoria, o processo é mais eficaz pois as informações sobre a RDM podem ser extraídas pelo CRM Dynamics nos respectivos relatórios, não mais em imagens.

Junto a essa melhoria para a localização das evidências, há o relatório individual da RDM disponível na Localização Avançada que apresenta os campos da RDM no CRM Dynamics que são auditados, substituindo várias capturas de tela que eram coletados separadamente, trazendo agilidade na coleta.

Outra novidade são os novos relatórios disponibilizados para fazer a gestão das mudanças abertas pelas equipes responsáveis por sistemas comerciais. Para atender a SOX, foram criados relatórios que apresentam todas as RDMs criadas em determinado período, que consideram o grupo de suporte e os assuntos relacionados ao CCS.

### 5.3 ORIENTAÇÃO AOS USUÁRIOS

Para eficácia do processo, os usuários envolvidos devem ser orientados sobre o novo processo. Tanto a equipe de Governança de TI quanto os analistas envolvidos na criação e atendimento da RDM devem ser orientados sobre a MMS juntamente com o novo processo para ficar claro o papel de cada um no registro das evidências da SOX durante o ciclo de vida de uma RDM.

Após a conclusão deste treinamento e forte divulgação do material para todos os envolvidos na TI, o processo pode ser utilizado pelos envolvidos no transporte de RDMs para o ambiente de produção do CCS.

As ações tomadas pela Governança de TI com os responsáveis quando as evidências estão falhas não fazem parte do escopo deste trabalho, mas, os analistas da equipe de governança podem e devem contatar quem falhou no procedimento, podendo inclusive adverti-lo para evitar próximos casos. Atualmente esta ação já é tomada quando necessário.

### 5.4 CONSIDERAÇÕES FINAIS

Neste capítulo foram apresentados o processo proposto por este trabalho, as diferenças existentes entre os processos apresentados e uma seção sobre a orientação prévia que os usuários envolvidos devem receber para a implantação desta solução.

O processo foi desenhado respeitando a metodologia MMS utilizada pelo Grupo CPFL. Para a definição do processo foi considerado o fluxo de trabalho que passa a RDM no CRM Dynamics e as evidências que devem ser registradas em cada ponto de controle referente às RDMs. O desenho dos processos e a descrição das atividades sofreram alterações durante o desenvolvimento do trabalho com o surgimento de novas alternativas para tornar as ações dos analistas de TI mais assertivas. Esta atividade resultou em um melhor entendimento da realização da auditoria da SOX nas RDMs.

Caso a equipe de auditoria queira que acompanhar o procedimento de forma assistida, conforme proposto por Gil (1999) na seção 2.4, o auditor pode agendar essa atividade com a governança de TI e presenciar a criação, atendimento e conclusão de uma RDM. Esta técnica é utilizada para aumentar a credibilidade das evidências coletadas.

Através da auditoria assistida, o auditor pode constatar, por exemplo, que quando a RDM já está concluída, os analistas de TI não conseguem fazer nenhuma alteração nos dados

presentes na mesma, não sendo possível alterar uma evidência.

No próximo capítulo deste trabalho, o processo desenhado será testado no ambiente da própria CPFL, simulando o ciclo de vida das RDMs, através de cenários de testes com diferentes possibilidades.

## 6 TESTE E VALIDAÇÃO DO PROCESSO

Este capítulo apresenta testes e validações do processo de geração de evidências no ambiente da CPFL e uma avaliação dos resultados obtidos nesses testes.

A validação da RDM acontece em cenários distintos, apresentando o ciclo de vida da RDM até seus diferentes estados conclusivos. Os cenários de testes estão descritos em tabelas que seguem o padrão do plano de testes do Grupo CPFL. O CRM Dynamics será utilizado em seu ambiente de qualidade, acessado pela rede interna da CPFL.

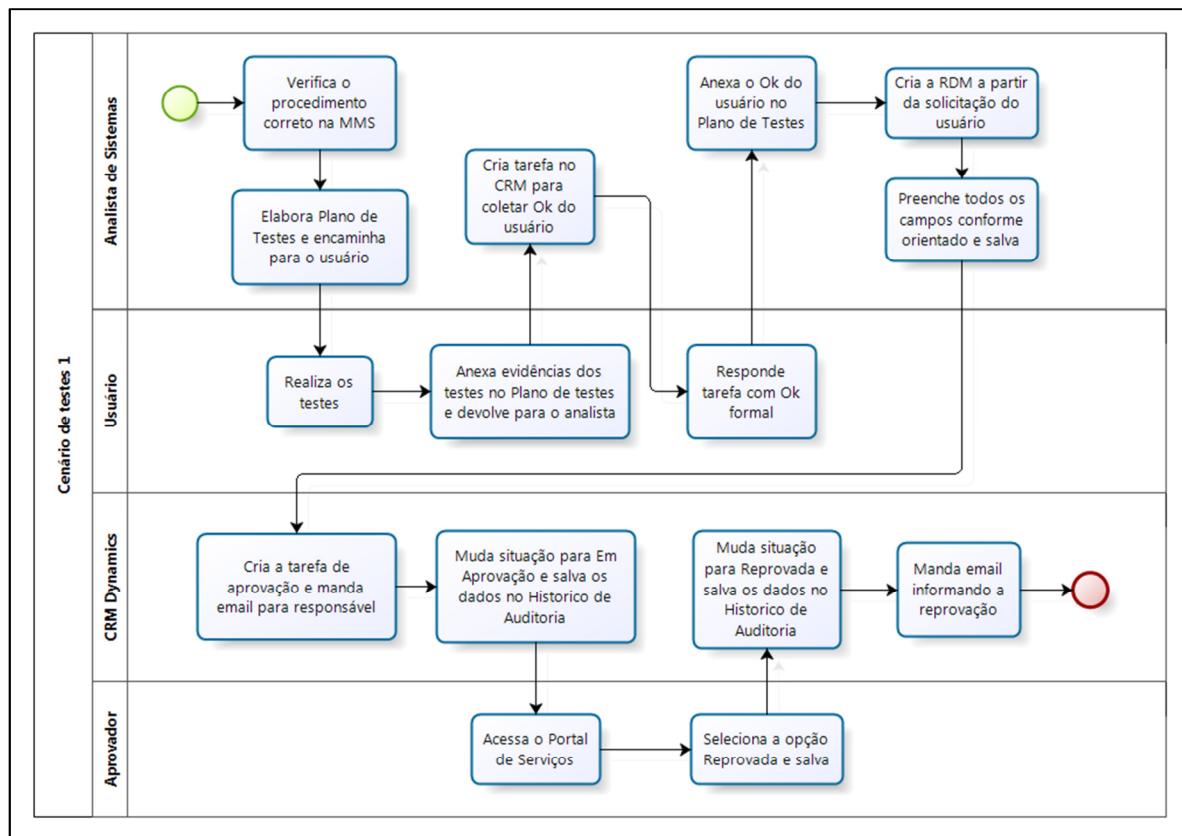
Os cenários de testes partem do princípio que a alteração realizada no ambiente de testes está de acordo com o esperado pela área de negócio. A seção 6.1 apresenta o cenário de teste de uma RDM concluída como Reprovada, a 6.2 apresenta os testes em uma RDM Cancelada, a 6.3 apresenta uma RDM Não Atendida e a seção 6.4 apresenta de uma RDM Atendida.

O Apêndice A apresenta capturas de tela que mostram passos executados durante os cenários de testes descritos.

### 6.1 CENÁRIO DE TESTES 1

Neste cenário de testes são apresentados os passos seguidos em um exemplo onde a RDM é encerrada como Reprovada. A figura 26 apresenta a demonstração gráfica do fluxo de execução do teste deste cenário e a tabela 5 apresenta os passos executados pela equipe de TI.

Figura 26 - Fluxo do Cenário de Testes 1



Fonte: Elaborado pelo autor

Tabela 5 - Passos do Cenário de Testes 1

(continua)

Seq.	Caso de Teste	Resultado Esperado
1	O analista de sistemas verifica o procedimento correto para criação da RDM e elabora o plano de testes.	O plano de testes elaborado conforme orientado, com os cenários de testes para que o usuário valide a alteração no ambiente de testes.
2	O usuário realiza os testes e faz o registro dos testes realizados conforme descrito no plano de testes, devolvendo-o para o analista de sistemas com seu ok.	O plano de testes devidamente preenchido com as evidências dos testes realizados.
3	O analista de sistemas cria tarefa solicitando formalização do usuário sobre a homologação no CRM Dynamics.	Tarefa para formalização criada no CRM Dynamics e direcionada para o usuário poder responder no Portal de Serviços.
4	O usuário responde a tarefa no Portal de Serviços, concluindo a sua homologação.	Registro do usuário com a homologação no CRM Dynamics para consultas posteriores.

(conclusão)

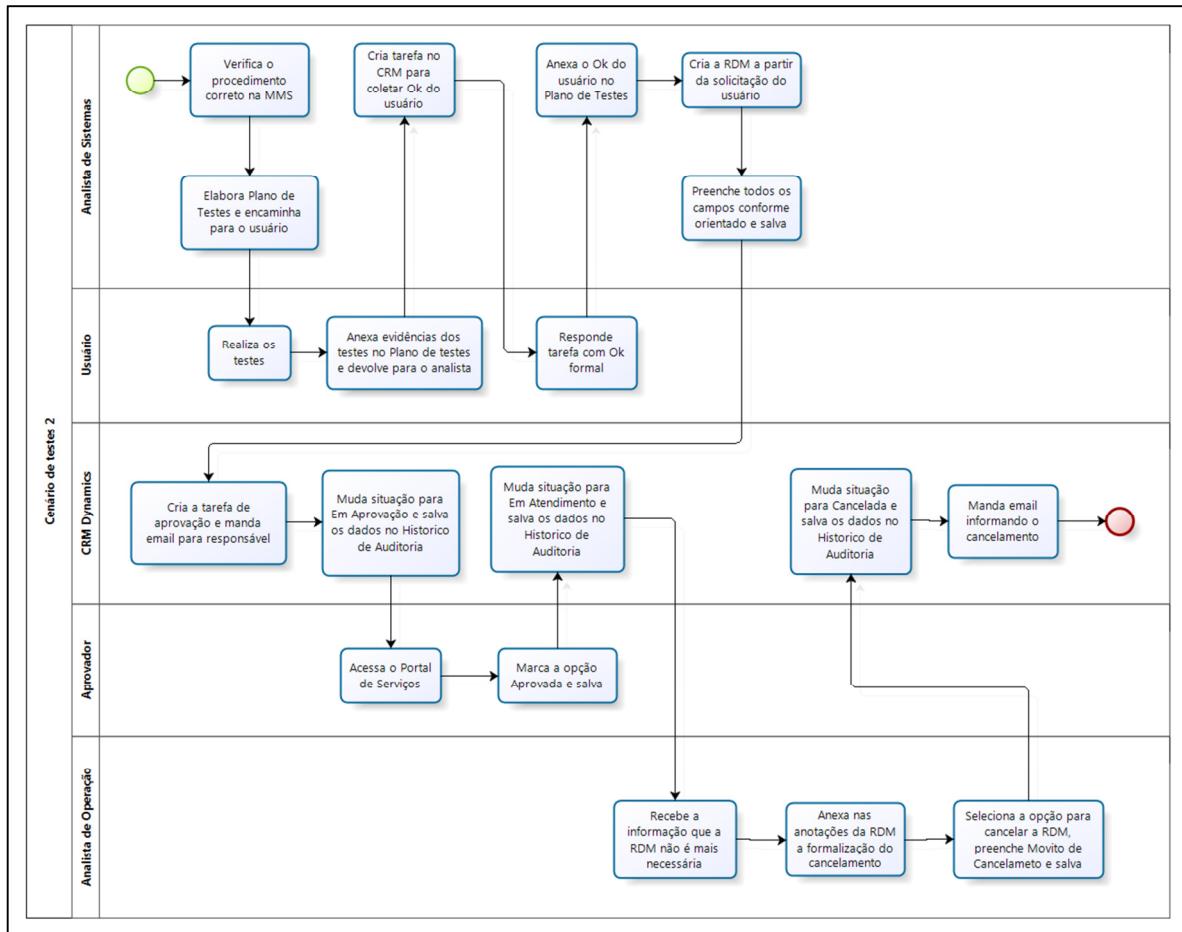
<b>Seq.</b>	<b>Caso de Teste</b>	<b>Resultado Esperado</b>
5	O analista de sistemas faz uma captura de tela da atividade respondida para incluir no plano de testes.	Conclusão do plano de testes, permitindo a criação da RDM para o transporte da alteração para o ambiente de produção.
6	O analista de sistemas cria a RDM a partir da solicitação do usuário com os campos auditados devidamente preenchidos.	Campos do formulário da RDM auditados preenchidos com as informações necessárias para o atendimento da mesma, mantendo vínculo com a solicitação do usuário.
7	O CRM Dynamics cria a tarefa de aprovação da RDM e avisa o usuário responsável da aprovação.	Tarefa de aprovação da RDM disponível para o responsável no Portal de Serviços.
8	O responsável pela aprovação acessa o Portal de Serviços e repara a RDM.	RDM reprovada, usuários envolvidos avisados por email e todos os registros salvos no Histórico de Auditoria da RDM.

Fonte: Elaborado pelo autor

## 6.2 CENÁRIO DE TESTES 2

Neste cenário de testes são apresentados os passos seguidos em um exemplo onde a RDM é encerrada como Cancelada. A figura 27 apresenta a demonstração gráfica do fluxo de execução do teste deste cenário e a tabela 6 apresenta os passos executados pela equipe de TI.

Figura 27 - Fluxo do Cenário de Testes 2



Fonte: Elaborado pelo autor

Tabela 6 - Passos do Cenário de Testes 2

(continua)

Seq.	Caso de Teste	Resultado Esperado
1	O analista de sistemas verifica o procedimento correto para criação da RDM e elabora o plano de testes.	O plano de testes elaborado conforme orientado, com os cenários de testes para que o usuário valide a alteração no ambiente de testes.
2	O usuário realiza os testes e faz o registro dos testes realizados conforme descrito no plano de testes, devolvendo-o para o analista de sistemas com seu ok.	O plano de testes devidamente preenchido com as evidências dos testes realizados.
3	O analista de sistemas cria tarefa solicitando formalização do usuário sobre a homologação no CRM Dynamics.	Tarefa para formalização criada no CRM Dynamics e direcionada para o usuário poder responder no Portal de Serviços.

(conclusão)

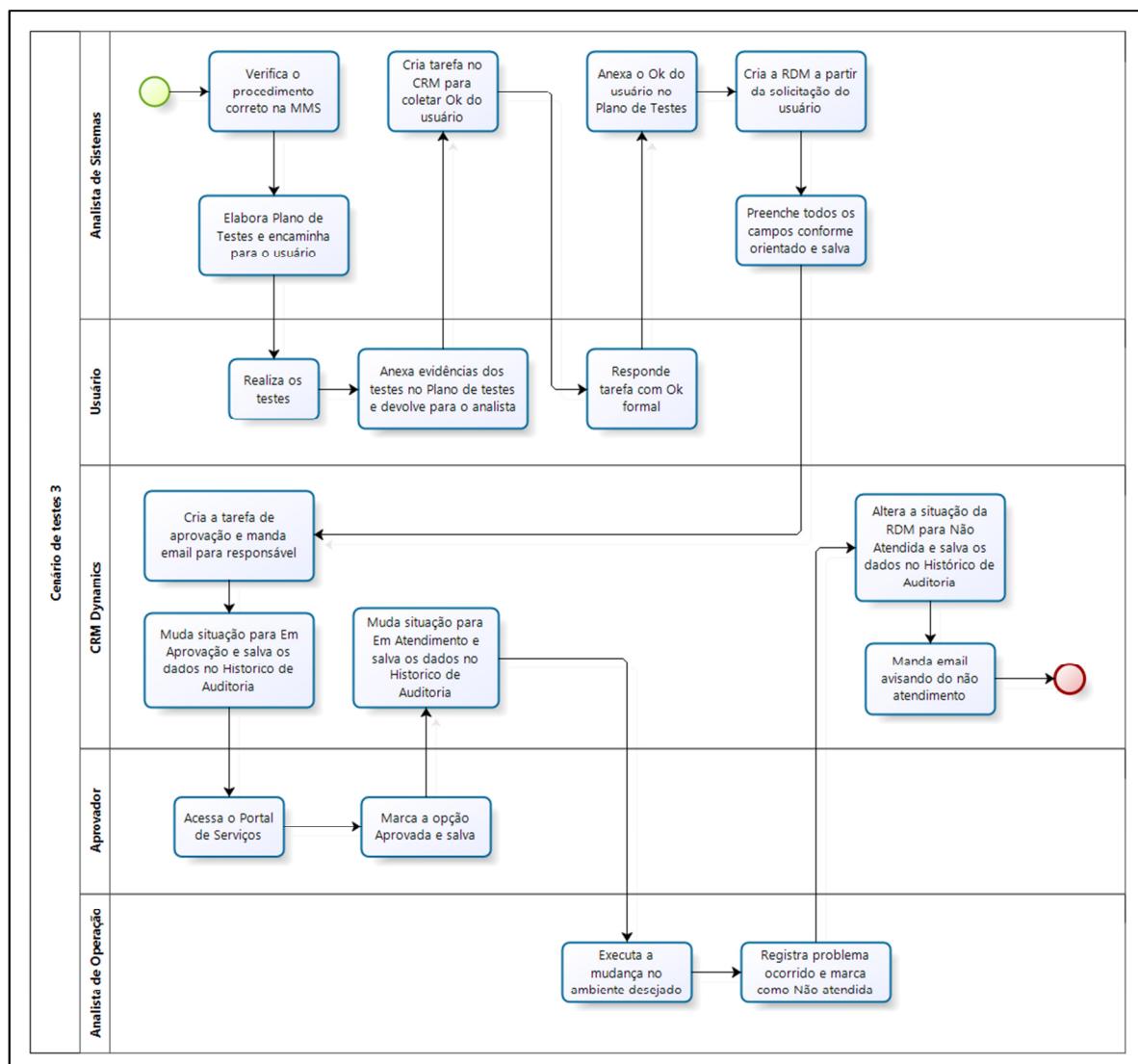
<b>Seq.</b>	<b>Caso de Teste</b>	<b>Resultado Esperado</b>
4	O usuário responde a tarefa no Portal de Serviços, concluindo a sua homologação.	Registro do usuário com a homologação no CRM Dynamics para consultas posteriores.
5	O analista de sistemas faz uma captura de tela da atividade respondida para incluir no plano de testes.	Conclusão do plano de testes, permitindo a criação da RDM para o transporte da alteração para o ambiente de produção.
6	O analista de sistemas cria a RDM a partir da solicitação do usuário com os campos auditados devidamente preenchidos.	Campos do formulário da RDM auditados preenchidos com as informações necessárias para o atendimento da mesma, mantendo vínculo com a solicitação do usuário.
7	O CRM Dynamics cria a tarefa de aprovação da RDM e avisa o usuário responsável da aprovação.	Tarefa de aprovação da RDM disponível para o responsável no Portal de Serviços.
8	O responsável pela aprovação acessa o Portal de Serviços e aprova a RDM.	RDM aprovada e encaminhada para atendimento da equipe de operação.
9	O analista de operação recebe a informação formal que a RDM não é mais necessária e pode ser cancelada e anexa na RDM.	Registro de cancelamento da RDM anexado nas Anotações da mesma para consultas posteriores.
10	O analista de operação seleciona a opção para cancelamento da RDM, preenche o motivo de cancelamento e salva a RDM.	RDM cancelada, usuários envolvidos avisados por email e todos os registros salvos no Histórico de Auditoria da RDM.

Fonte: Elaborado pelo autor

### 6.3 CENÁRIO DE TESTES 3

Neste cenário de testes são apresentados os passos seguidos em um exemplo onde a RDM é encerrada como Não Atendida. A figura 28 apresenta a demonstração gráfica do fluxo de execução do teste deste cenário e a tabela 7 apresenta os passos executados pela equipe de TI.

Figura 28 - Fluxo do Cenário de Testes 3



Fonte: Elaborado pelo autor

Tabela 7 - Passos do Cenário de Testes 3

(continua)

Seq.	Caso de Teste	Resultado Esperado
1	O analista de sistemas verifica o procedimento correto para criação da RDM e elabora o plano de testes.	O plano de testes elaborado conforme orientado, com os cenários de testes para que o usuário valide a alteração no ambiente de testes.
2	O usuário realiza os testes e faz o registro dos testes realizados conforme descrito no plano de testes, devolvendo-o para o analista de sistemas com seu ok.	O plano de testes devidamente preenchido com as evidências dos testes realizados.

(conclusão)

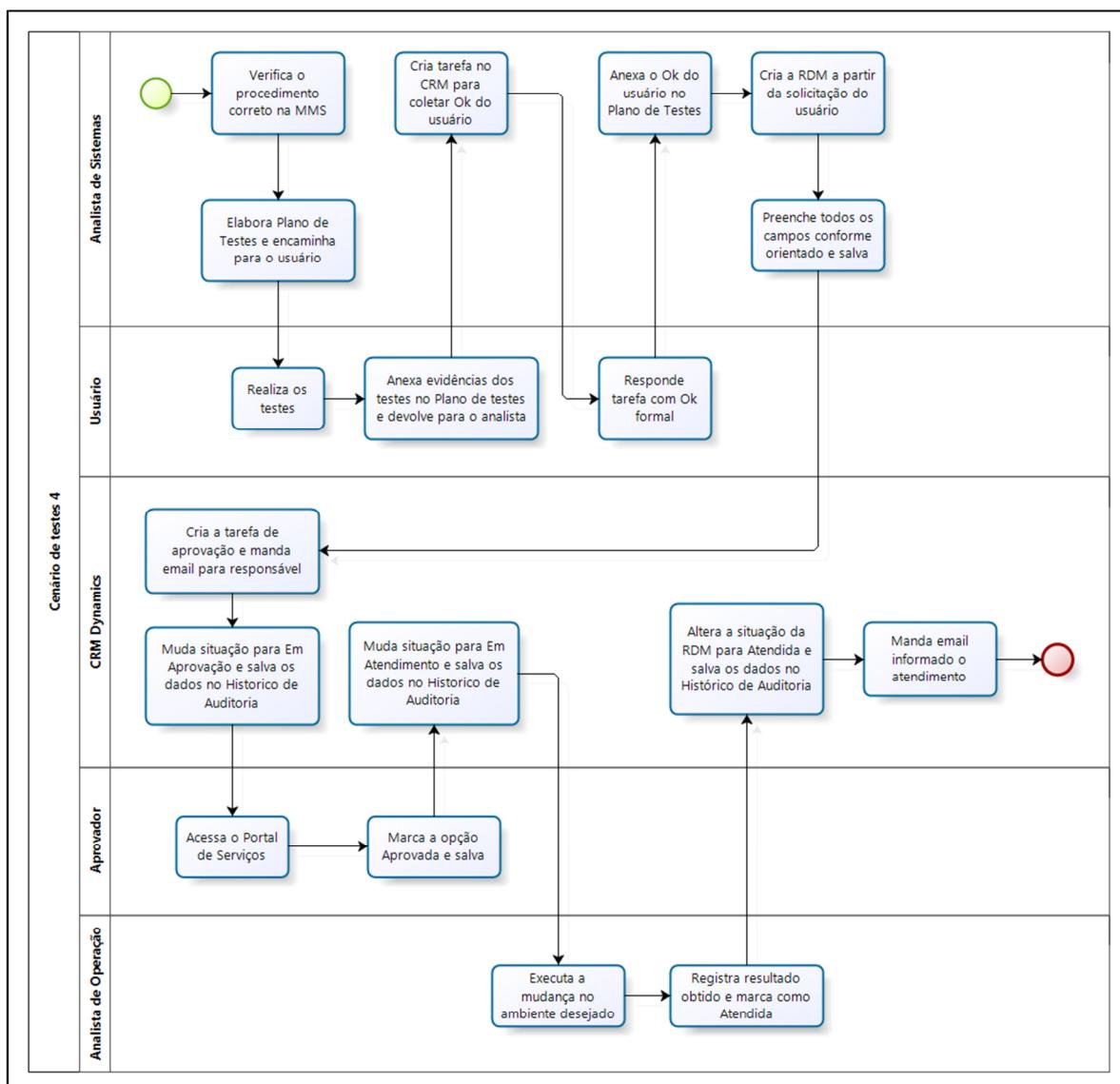
<b>Seq.</b>	<b>Caso de Teste</b>	<b>Resultado Esperado</b>
3	O analista de sistemas cria tarefa solicitando formalização do usuário sobre a homologação no CRM Dynamics.	Tarefa para formalização criada no CRM Dynamics e direcionada para o usuário poder responder no Portal de Serviços.
4	O usuário responde a tarefa no Portal de Serviços, concluindo a sua homologação.	Registro do usuário com a homologação no CRM Dynamics para consultas posteriores.
5	O analista de sistemas faz uma captura de tela da atividade respondida para incluir no plano de testes.	Conclusão do plano de testes, permitindo a criação da RDM para o transporte da alteração para o ambiente de produção.
6	O analista de sistemas cria a RDM a partir da solicitação do usuário com os campos auditados devidamente preenchidos.	Campos do formulário da RDM auditados preenchidos com as informações necessárias para o atendimento da mesma, mantendo vínculo com a solicitação do usuário.
7	O CRM Dynamics cria a tarefa de aprovação da RDM e avisa o usuário responsável da aprovação.	Tarefa de aprovação da RDM disponível para o responsável no Portal de Serviços.
8	O responsável pela aprovação acessa o Portal de Serviços e aprova a RDM.	RDM aprovada e encaminhada para atendimento da equipe de operação.
9	O analista de operação tenta executar a alteração conforme solicitado, porém acontece um problema no atendimento, aplicando o plano de retorno se necessário, registra o problema ocorrido e salva a RDM como não atendida.	RDM concluída como não atendida, usuários envolvidos avisados por email e todos os registros salvos no Histórico de Auditoria da RDM.

Fonte: Elaborado pelo autor

## 6.4 CENÁRIO DE TESTES 4

Neste cenário de testes são apresentados os passos seguidos em um exemplo onde a RDM é encerrada como Atendida. A figura 29 apresenta a demonstração gráfica do fluxo de execução do teste deste cenário e a tabela 8 apresenta os passos executados pela equipe de TI.

Figura 29 - Fluxo do Cenário de Testes 4



Fonte: Elaborado pelo autor

Tabela 8 - Passos do Cenário de Testes 4

(continua)

Seq.	Caso de Teste	Resultado Esperado
1	O analista de sistemas verifica o procedimento correto para criação da RDM e elabora o plano de testes.	O plano de testes elaborado conforme orientado, com os cenários de testes para que o usuário valide a alteração no ambiente de testes.
2	O usuário realiza os testes e faz o registro dos testes realizados conforme descrito no plano de testes, devolvendo-o para o analista de sistemas com seu ok.	O plano de testes devidamente preenchido com as evidências dos testes realizados.

(conclusão)

<b>Seq.</b>	<b>Caso de Teste</b>	<b>Resultado Esperado</b>
3	O analista de sistemas cria tarefa solicitando formalização do usuário sobre a homologação no CRM Dynamics.	Tarefa para formalização criada no CRM Dynamics e direcionada para o usuário poder responder no Portal de Serviços.
4	O usuário responde a tarefa no Portal de Serviços, concluindo a sua homologação.	Registro do usuário com a homologação no CRM Dynamics para consultas posteriores.
5	O analista de sistemas faz uma captura de tela da atividade respondida para incluir no plano de testes.	Conclusão do plano de testes, permitindo a criação da RDM para o transporte da alteração para o ambiente de produção.
6	O analista de sistemas cria a RDM a partir da solicitação do usuário com os campos auditados devidamente preenchidos.	Campos do formulário da RDM auditados preenchidos com as informações necessárias para o atendimento da mesma, mantendo vínculo com a solicitação do usuário.
7	O CRM Dynamics cria a tarefa de aprovação da RDM e avisa o usuário responsável da aprovação.	Tarefa de aprovação da RDM disponível para o responsável no Portal de Serviços.
8	O responsável pela aprovação acessa o Portal de Serviços e aprova a RDM.	RDM aprovada e encaminhada para atendimento da equipe de operação.
9	O analista de operação executa a alteração no ambiente de produção conforme solicitado, registra o resultado e salva a RDM como atendida.	RDM concluída como atendida, usuários envolvidos avisados por email e todos os registros salvos no Histórico de Auditoria da RDM.

Fonte: Elaborado pelo autor

## 6.5 AVALIAÇÃO DOS RESULTADOS OBTIDOS

Os resultados obtidos com os testes são positivos, pois atenderam o proposto no trabalho. Com a geração das evidências neste formato, quando for realizada uma auditoria, é possível coletar as evidências da seguinte forma:

- Informações da RDM individual: pelo relatório criado no CRM Dynamics, podendo ser validadas as informações pelo Histórico de Auditoria da mesma;
- Homologação: pelo documento anexado nas anotações da RDM com o aceite do usuário, podendo ser validado no próprio CRM Dynamics;
- Aprovação da RDM: pelo relatório criado no CRM Dynamics, podendo ser

validadas as informações pelo Histórico de Auditoria da tarefa de aprovação, que terá documentos anexos se necessário;

- Revisão pós-implementação: pelo email encaminhado automaticamente pelo CRM Dynamics, sendo que este pode ser exportado para um arquivo do tipo pdf, dificultando alterações;
- Controles das mudanças: através dos relatórios criados, é possível a verificação de todas as RDMs criadas e já concluídas referentes ao sistema CCS no período auditado;
- Metodologia de manutenção de sistemas: a própria MMS, que também é uma evidência auditada, pode ser exportada pelo GED CPFL;
- Implementadores de RDMs: pelo relatório criado no CRM Dynamics, que mostra os implementadores de RDMs no período auditado;
- Histórico de Auditoria: para garantir a veracidade das informações inseridas na RDM, fornecendo mais credibilidade às evidências coletadas.

## 6.6 CONSIDERAÇÕES FINAIS

Este capítulo apresentou diferentes cenários de teste para validação do processo proposto no capítulo 5. Foram simulados quatro testes de acordo com as possíveis formas de conclusão de uma RDM. O processo se mostrou eficaz para atender os pontos de controle apresentados pela governança de TI.

Este capítulo apresentou também uma avaliação dos resultados obtidos nos testes realizados, onde são apresentadas as evidências que podem ser coletadas, e sua forma, em uma possível auditoria.

O próximo capítulo deste trabalho apresenta a conclusão do mesmo e as sugestões de trabalhos futuros no ambiente de TI do Grupo CPFL.

## 7 CONCLUSÃO

Este trabalho demonstrou a criação de um processo que respeita as boas práticas de auditoria e atende as necessidades que a empresa CPFL tem quanto a geração de evidências nas mudanças em sistemas comerciais, sendo este processo compatível com a MMS utilizada pelas equipes na TI.

Primeiramente foi realizado o levantamento do referencial teórico onde foram estudados conceitos de auditoria, técnicas e práticas para realizá-la. Este referencial foi importante para compreender a metodologia utilizada pela empresa e no entendimento da melhor forma de construção do processo criado neste trabalho.

O bom entendimento da auditoria, da Lei SOX e dos pontos de controle presentes na implantação de SI contribuíram para construção do processo em BPMN. A forma como o registro das evidências durante o ciclo de vida da RDM ocorre atualmente foi ajustada no desenho do processo para tornar a geração das evidências mais assertiva, não sendo contraditória a MMS utilizada na CPFL.

O ambiente da CPFL foi estudado para compreender onde são criadas e encerradas as RDMs e porque elas são necessárias. A metodologia também foi estudada, junto a forma como ocorre todo o processo que envolve as RDMs, utilizadas para a manutenção no CCS, sistema comercial utilizado pelo grupo.

Os analistas não são devidamente orientados sobre como devem proceder na criação e atendimento das RDMs, o que justifica as falhas encontradas. A falta das evidências para atender os pontos de controle do grupo CPFL é uma grande preocupação da governança de TI, visto que nas auditorias externas, causam um impacto negativo nos relatórios gerados. Definir mais os processos, como feito neste trabalho, pode auxiliar a governança em mitigar as falhas perante as empresas contratadas para auditoria.

O processo foi desenhado conforme as evidências solicitadas nos referenciais estudados. Com a utilização dos diagramas propostos fica claro que, caso as evidências sejam registradas no local correto, a posterior coleta delas quando necessário é relativamente simples. Mas, sem isto, a MMS não é específica sobre quando e como as evidências devem ser registradas.

Com os novos relatórios propostos, fica mais fácil a identificação das falhas na realização dos registros nas RDMs. Através dos relatórios que mostram os campos auditados mostram de forma clara os problemas existentes na geração das evidências na criação e

encerramento das RDMs.

Com a publicação de novas orientações sobre o processo de geração de evidências no GED CPFL, um comunicado para as equipes envolvidas e a devida orientação para as equipes envolvidas, os analistas da TI terão conhecimento sobre a forma correta de fazer os registros, diminuindo o número de falhas.

Para realização de testes, foram simulados no ambiente de qualidade, diferentes cenários, com diferentes RDMs, em ciclos de vida com términos diferentes. Até então o processo ainda sofreu ajustes e melhorias, conforme surgiam novas necessidades e verificações. O processo desenhado se mostrou eficaz nos cenários, demonstrando que o objetivo do trabalho foi alcançado.

## 7.1 TRABALHOS FUTUROS

Com o desenvolvimento deste trabalho de conclusão, os seguintes pontos foram levantados como sugestão para melhorias futuras:

- A criação de um processo de coleta de evidências semelhante ao deste trabalho também para a Metodologia de Desenvolvimento de Projetos de Sistemas (MDPS);
- Obrigatoriedade de preenchimento dos campos de vínculo com solicitação do usuário no processo de criação da RDM, uma vez que o preenchimento do campo atualmente não é obrigatório, mas é previsto pelo processo proposto neste trabalho;
- Melhoria no CRM Dynamics para permitir que o Histórico de Auditoria seja extraído através da própria ferramenta, uma vez que atualmente o Histórico de Auditoria precisa ser extraído a partir de uma consulta efetuada diretamente no banco de dados do CRM Dynamics.

## REFERÊNCIAS

- ABNT. NBR ISO/IEC 27005: **Tecnologia da Informação – Técnicas de Segurança – Gestão de riscos de segurança da informação.** 1<sup>a</sup> Edição. Rio de Janeiro: ABNT, 2008.
- ATTIE, William. **Auditoria: conceitos e aplicações.** 5<sup>a</sup> Edição. São Paulo: Editora Atlas, 2010.
- BRANDALISE, Mauricio Modesto Toscan. **ROTEIRO PARA ELABORAÇÃO DE PROGRAMAS DE AUDITORIA EM SISTEMA ERP (ENTERPRISE RESOURCE PLANNING).** 2012. 102 f. Trabalho de Conclusão de Curso - Universidade de Caxias do Sul, Bacharelado em Sistemas de Informação, Caxias do Sul, 2012.
- CHEN, Wei; SMIELIAUSKAS, Wally J; TRIPPEN, Gerhard. **An Audit Evidence Gathering Model in Online Auditing Environments.** Waikoloa, Havai: IEEE, 2007.
- FERNANDES, Aguinaldo Aragon. **Implantando a governança de TI: da estratégia à gestão dos processos e serviços /** Aguinaldo Aragon Fernandes, Vladimir Ferraz de Abreu. Rio de Janeiro: Brasport, 2006.
- GIL, Antonio de Lourenço. **Auditoria de computadores.** 4<sup>a</sup> Edição. São Paulo: Editora Atlas, 1999.
- GUIMARÃES, Thiago Tomáz Pereira. **Controles Internos na Tesouraria de uma Empresa do Setor Elétrico.** 2010. 71 f. Monografia - Universidade Federal de Santa Catarina, Curso de Ciências Contábeis, Florianópolis, 2010.
- IMONIANA, Joshua Onome. **Auditoria de Sistemas de Informação.** 2<sup>a</sup> Edição. São Paulo: Editora Atlas, 2008.
- ISACA. **CISA Review Manual 2011.** Estados Unidos da América, 2011.
- IT GOVERNANCE INSTITUTE. **COBIT 4.1.** Estados Unidos da América, 2007.
- JUND, Sergio. **Auditoria: conceitos, normas técnicas e procedimentos: teoria e 600 questões – Estilo ESAF, UNB e outras.** 4<sup>a</sup> Edição. Rio de Janeiro: Editora Impetus, 2002.
- LORANDI, Angela. **Projeto de Pesquisa: Implantação de Ferramenta Qualitor e as Melhores Práticas do ITIL na empresa Lojas Colombo S.A.** 2009. 79 f. Trabalho de Conclusão - Faculdade TecBrasil, Curso Superior de Tecnologia em Gestão de Ambientes Computadorizados, Caxias do Sul, 2009.
- LYRA, Maurício Rocha. **Segurança e Auditoria em Sistemas de Informação.** Rio de Janeiro: Editora Ciência Moderna, 2008.
- MAGALHÃES, Ivan Luizio. **Gerenciamento de Serviços de TI na prática: uma abordagem com base na ITIL: inclui ISO/IEC 20.000 e IT Flex.** Série Gerenciamento de TI. São Paulo: Editora Novatec, 2007.

MICROSOFT Dynamics CRM 2011, versão 5.0. [S.l.]: Microsoft Corporation, 2011. Licenciado para a organização: CPFL Energia MSCRM.

MURATORE, Claudia Regina. **Customização do Sistema Comercial da RGE e Certificação SOX**. 2012. 7 f. Estágio Curricular - Universidade de Caxias do Sul, Bacharelado em Sistemas de Informação, Caxias do Sul, 2012.

NETO, Bruno Jacob Gomes. **Análise dos Impactos da Implantação da Governança em Tecnologia da Informação em uma Empresa de Energia na Perspectiva da Equipe de TI**. 2012. 156 f. Dissertação de Mestrado Profissional - Universidade Federal Fluminense, Niterói, 2012.

PETERS, Marcos. **Implantando e gerenciando a Lei Sarbanes Oxley**. São Paulo: Editora Atlas, 2007.

PIZZOLI, Fábio Antonio. **Sistema de Gerenciamento de Segurança de Informações: Processo de Auditoria**. 2004. 135 f. Trabalho de Conclusão de Curso de Mestrado Profissionalizante em Engenharia - Universidade Federal do Rio Grande do Sul, Porto Alegre, 2004.

RGE – Uma empresa CPFL Energia. **Quem somos**, disponível em <<http://www.rge-rs.com.br/ARGE/QuemSomos/tabid/116/language/pt-BR/Default.aspx>>, acessado em 15/08/2013.

\_\_\_\_\_. **Relatório de Gestão 2010 RGE – Uma empresa CPFL Energia**. PNQ – Programa Nacional de Qualidade, RGE, 2010.

SOUZA, Rodrigo Gargioni de. **Lei Sarbanes-Oxley, Auditoria e Fraudes**. 2004. 152 f. Projeto de Conclusão de Estágio - Universidade Federal de Santa Catarina, Florianópolis, 2004.

TESSARI, Rogério. **Gestão de processos de negócio: um estudo de caso da BPMN em uma empresa do setor moveleiro**. 2008. 91 f. Dissertação (Mestrado) – Universidade de Caxias do Sul, Programa de Pós-Graduação em Administração, Caxias do Sul, 2008.

WEILL, Peter; ROSS, Jeane W. **Governança de TI, Tecnologia da Informação**. São Paulo: M Books do Brasil Editora, 2006.

## ANEXO A – RELATÓRIO DE RDMS ATENDIDAS

Este anexo apresenta um exemplo de Relatório para Auditoria SOX - Atendidas exportado do CRM Dynamics no ambiente de produção.

<b>Id da Mudança</b>	<b>Grupo de Suporte</b>	<b>Proprietário</b>	<b>Data de Criação</b>	<b>Razão do Status</b>	<b>Origem da RDM</b>	<b>Aprovador 1:</b>	<b>Data de Aprovação1:</b>	<b>Comentário da Implementação</b>	<b>Data Real de Implementação</b>	<b>Implementado Por</b>	<b>Descrição do Impacto</b>	<b>Riscos Associados</b>	<b>Plano de Retorno</b>
RDM-0033826	TI_SAPCC S_Basis	Patrícia Viviane Xavier	03/03/2015 14:03	Atendida	Gestão de Mudanças	Leandro dos Santos Melo	03/03/2015 14:41	Requests transportadas com sucesso.	04/03/2015	Henrique Vitorino Grota	Valores errados no relatório de Serviços Regulados .	Valores errados no relatório de Serviços Regulados .	Desfazer as configurações na Query QFAT_FAT 012
RDM-0035014	TI_SAPCC S_Basis	Patrícia Viviane Xavier	28/04/2015 14:27	Atendida	Gestão de Mudanças	Leandro dos Santos Melo	28/04/2015 17:03	Transportar para o BIP as requests a baixo seguindo a ordem listada.	29/04/2015	Henrique Vitorino Grota	Dados incorretos.	Dados incorretos nos relatórios de demanda	Voltar a versão antiga da transformação alterada.
RDM-0035867	TI_SAPCC S_Basis	Fabiana Salomao Ferreira	10/06/2015 10:25	Atendida	Gestão de Mudanças	Heloisa Helena Oranges Teixeira	10/06/2015 17:54	Realizado o import das requests conforme solicitado.	11/06/2015	Vinicio Valerio Candiani	Exibição de NoDunning para faturas que não possuem o bloqueio na tabela controle de base de inadimplência.	Indisponibilidade temporária do programa de base de clientes inadimplentes (ZCCSAC CR0111)	Acionar o analista responsável - Fabiana Ferreira

## ANEXO B – RELATÓRIO DE RDMS CANCELADAS

Este anexo apresenta um exemplo do Relatório para Auditoria SOX - Canceladas exportado do CRM Dynamics no seu ambiente de produção.

<b>Id da Mudan-ça</b>	<b>Grupo de Suporte</b>	<b>Data de Criação</b>	<b>Razão do Status</b>	<b>Motivo de Cancelamento</b>	<b>Origem da RDM</b>	<b>Aprova-dor 1:</b>	<b>Data de Aprova-ção1:</b>	<b>Descrição do Impacto</b>	<b>Riscos Asso-ciados</b>	<b>Plano de Re-torno</b>
RDM-0032682	TI_SAPCCS_Basis	30/12/2014 15:27	Cancelada	RDM aberta indevidamente Atenciosamente André Amorim	Gestão de Demandas	Carlos Eduardo De Azeredo	30/12/2014 15:40	CANCELADO	CANCELADO	RDM-0032682
RDM-0032006	TI_SAPCCS_Basis	24/11/2014 14:22	Cancelada	RDM aberta sem o numero da request.	Gestão de Mudanças	Elaine Patricia Quaresma Xavier	25/11/2014 10:39	problemas com os filtros do relatório	N/A - Não há nenhum risco associado	RDM-0032006
RDM-0031140	TI_SAPCCS_Basis	10/10/2014 11:48	Cancelada	Request aberta indevidamente. Está sendo cancelada.	Gestão de Demandas	Jose Abimael de Lima	10/10/2014 11:56	Request aberta indevidamente. Está sendo cancelada.	Request aberta indevidamente. Está sendo cancelada.	RDM-0031140
RDM-0030246	TI_SAPCCS_Basis	29/08/2014 15:24	Cancelada	CANCELAR RDM. A RDM FOI CRIADA ERRADA!	Gestão de Demandas	Jose Abimael de Lima	29/08/2014 15:47	A RDM FOI CRIADA ERRADA!	A RDM FOI CRIADA ERRADA!	RDM-0030246

## ANEXO C – RELATÓRIO DE RDMS GERAL

Este anexo apresenta um exemplo do Relatório para Auditoria SOX - Geral exportado no CRM Dynamics no seu ambiente de produção.

<b>Id da Mudança</b>	<b>Grupo de Suporte</b>	<b>Data de Criação</b>	<b>Razão do Status</b>	<b>Origem da RDM</b>	<b>Aprovador 1:</b>	<b>Data de Aprovação1:</b>	<b>Descrição do Impacto</b>	<b>Riscos Associados</b>	<b>Comentário da Implementação</b>	<b>Data Real de Implementação</b>	<b>Implementado Por</b>	<b>Motivo de Cancelamento</b>	<b>Plano de Retorno</b>
RDM-0032324	TI_SAPCCS_Basis	10/12/2014 11:25	Atendida	Gestão de Demandas	Carlos Eduardo De Azeredo	10/12/2014 17:04	Impacto na geração do reprocessamento de indicadores	Reprocessamento incorreto	Requests transportadas com sucesso.	11/12/2014	Henrique Vitorino Grota		RDM-0032324
RDM-0032198	TI_SAPCCS_Basis	03/12/2014 15:40	Atendida	Gestão de Mudanças	Sérgio Andrade de Siqueira Franco	04/12/2014 08:23	geração incorreta do arquivo com as leituras	layout incorreto do arquivo	Realizado o import da request conforme solicitado. RC = 0.	04/12/2014	Vinicius Valerio Candiani		RDM-0032198
RDM-0032006	TI_SAPCCS_Basis	24/11/2014 14:22	Cancelada	Gestão de Mudanças	Elaine Patricia Quaresma Xavier	25/11/2014 10:39	problemas com os filtros do relatório	N/A - Não há nenhum risco associado	Filtros do relatório de faturamento diário.	27/11/2014	Vinicius Valerio Candiani	RDM aberta sem o numero da request.	RDM-0032006

## ANEXO D – RELATÓRIO DE RDMS NÃO ATENDIDAS

Este anexo apresenta um exemplo do Relatório para Auditoria SOX - Não Atendidas exportado do CRM Dynamics no seu ambiente de produção.

<b>Id da Mudança</b>	<b>Grupo de Suporte</b>	<b>Data de Criação</b>	<b>Razão do Status</b>	<b>Origem da RDM</b>	<b>Aprovador 1:</b>	<b>Data de Aprovação1:</b>	<b>Comentário da Implementação</b>	<b>Data Real de Implementação</b>	<b>Implementado Por</b>	<b>Descrição do Impacto</b>	<b>Riscos Associados</b>	<b>Plano de Retorno</b>
RDM-0026289	TI_Operacao	13/02/2014 10:20	Não Atendida	Ocorrências	Marcos Miranda Vieira	13/02/2014 15:10	Aguardando aprovação para implementação da alteração.	14/02/2014	Alexandre Falvo	Com essa alteração, fatalmente a execução deste job invadirá a manha do domingo, causando lentidão no call center neste periodo	A execução deste job (SM_TEC_REORG_D_FKKLOCK_S_CCS) causa lentidão no call center.	Refazer alteração do horario de inicio
RDM-0027654	TI_SAPCCS_Basis	16/04/2014 09:39	Não Atendida	Ocorrências	João Alvaro Wolf Piton	16/04/2014 09:57	Transportar request abaixo.	17/04/2014	Fabiano Fernandes Alves	Baixo impacto no encerramento de notas	Não há riscos associados.	Voltar versão do BOR ZISUSMNOTI

## ANEXO E – RELATÓRIO DE RDMS REPROVADAS

Este anexo apresenta um exemplo do Relatório para Auditoria SOX - Reprovadas exportado do CRM Dynamics no seu ambiente de produção.

<b>Id da Mudança</b>	<b>Grupo de Suporte</b>	<b>Data de Criação</b>	<b>Razão do Status</b>	<b>Origem da RDM</b>	<b>Aprovador 1:</b>	<b>Data de Aprovação1:</b>	<b>Descrição do Impacto</b>	<b>Riscos Associados</b>	<b>Plano de Retorno</b>
RDM-0032747	TI_SAPCCS_Basis	06/01/2015 15:09	Reprovada	Gestão de Mudanças	Heloisa Helena Oranges Teixeira	13/01/2015 17:25	Caso a Mudança não seja atendida, os clientes poderão receber faturas com encargos incorretos.	Caso a Mudança não seja atendida, os clientes poderão receber faturas com encargos incorretos.	RDM-0032747
RDM-0028348	TI_SAPCCS_Basis	22/05/2014 15:15	Reprovada	Gestão de Mudanças	Heloisa Helena Oranges Teixeira	24/07/2014 18:00	Não efetivar o encontro de contas.	Não efetivar o encontro de contas.	RDM-0028348
RDM-0027039	TI_SAPCCS_Basis	20/03/2014 18:04	Reprovada	Ocorrências	Juçara Helena De Oliveira	07/05/2014 16:44	Impactos nas telas de fraude.	RDM cancelada.	RDM-0027039
RDM-0026874	TI_SAPCCS_Basis	14/03/2014 10:11	Reprovada	Ocorrências	Heloisa Helena Oranges Teixeira	20/03/2014 08:49	Caso a RDM não seja atendida o campo "Qtd Dias" apresentará dados incorretos.	Não se aplica.	RDM-0026874
RDM-0026024	TI_SAPCCS_Basis	31/01/2014 15:32	Reprovada	Gestão de Mudanças	Priscila Cazarini	10/04/2014 08:16	contabilização incorreta.	faturamento incorreto.	RDM-0026024

## ANEXO F – RELATÓRIO AUDITORIA SOX – IMPLEMENTADORES CCS

Este anexo apresenta o relatório criado para controle de implementadores de RDMs no CCS, exportado do CRM Dynamics. Este exemplo tem os usuários que implementaram RDM's no ano de 2015.

Nome Completo	Unidade de Negócio	Título	Modo de Acesso	Modo de Acesso Restrito
Bruno Rodrigues Lopes	Campinas	Analista Basis	Leitura-Gravação	Não
Fabiano Fernandes Alves	CPFLEnergiaMSCRM	Analista Basis	Leitura-Gravação	Não
Gabriel Carneiro	TI	Analista Nível 1	Leitura-Gravação	Não
Henrique Vitorino Grota	CPFLEnergiaMSCRM	Analista Basis	Leitura-Gravação	Não
Vinicius Valerio Candiani	TI - Serviços Corporativos	Analista Basis Pleno	Leitura-Gravação	Não

## ANEXO G – RELATÓRIO DE RDM INDIVIDUAL

Este anexo apresenta o Relatório para Auditoria SOX – RDM Individual criado para verificação de uma RDM específica, exportado do CRM Dynamics. Este exemplo tem a RDM-0033826, apresentando os campos necessários conforme este trabalho.

<b>Id da Mudança</b>	<b>Origem da RDM</b>	<b>Riscos Associados</b>	<b>Descrição do Impacto</b>	<b>Plano de Retorno</b>	<b>Aprovador 1:</b>	<b>Data de Aprovação1:</b>
RDM-0033826	Gestão de Mudanças	Valores errados no relatório de Serviços Regulados.	Valores errados no relatório de Serviços Regulados.	Desfazer as configurações na Query QFAT_FAT012	Leandro dos Santos Melo	03/03/2015 14:41

## ANEXO H – TEMPLATE DO PLANO DE TESTES DO GRUPO CPFL

Este anexo apresenta o template do Plano de Testes adotado como padrão no Grupo CPFL.

<b>PLANO DE TESTES</b>		
<b>DEM / Ocorrência</b>	<b>Título</b>	<b>Módulo</b>
<b>Número da demanda ou da ocorrência</b>	<b>Título da demanda ou ocorrência</b>	<b>Módulo do sistema</b>
<b>OBS: Padrão do nome do documento: Teste_Módulo_Descrição</b>		
<b>Depto./ Divisão</b>	<b>Dt. Elaboração</b>	<b>Sistema</b>
<b>Consultor</b>	<b>Analista</b>	
<b>Executante(s) dos Testes</b>		

<b>Check-list da Mudança</b>			
<b>Seq.</b>	<b>Seq.</b>	<b>Resposta</b>	<b>Observações</b>
1	Altera processo de negócio?		
2	Altera interface?		
3	É um novo módulo?		
4	A mudança exige carga de dados?		
5	É necessário Criptografia?		
6	É uma manutenção na aplicação (Sustain)?		

Para qualquer resposta positiva acima, testes específicos devem ser definidos em conjunto com os testes funcionais abaixo.

<b>Orientações</b>
O Plano de teste deve evidenciar a correção do incidente/problema ou a melhoria decorrente da Demanda.

As alterações/implementações devem passar por testes internos efetuados pelos consultores e enviado aos usuários para os testes funcionais.
Se os testes funcionais forem aprovados, inicia-se o processo de Mudança, caso contrário as alterações/implementações retornam aos consultores para ajustes.
Quando os testes forem aprovados é gerada a mudança a ser transportada para produção.
Os passos que compõem o Plano de teste, de acordo com a característica de cada mudança, devem ser descritos abaixo na tabela "Caso de Teste".
Quando se tratar de mudanças originadas de Demandas, estas devem ser homologadas pela equipe de TI, antes de serem enviadas para os usuários.

<b>Caso de Teste</b>				
<b>Seq.</b>	<b>Caso de Teste (descrição completa)</b>	<b>Resultado Esperado</b>	<b>OK?</b>	<b>Qtd. Erros</b>
1			OK	0
<b>Número Total de Erros Encontrados</b>				0

### **Prints de Telas dos Testes Realizados**

Anexar aqui as capturas de tela referentes aos testes realizados para homologação da alteração.

<b>Questionário de Aceitação</b>	
<b>Os testes realizados atendem os objetivos propostos?</b>	
<b>SIM</b>	
<b>Você está de acordo com os resultados apresentados?</b>	
<b>SIM</b>	
<b>A Demanda/Ocorrência pode ser concluída?</b>	
<b>SIM</b>	

### **Print do E-mail de Aceitação**

Anexar aqui a captura de tela com o aceite do usuário.

## APÊNDICE A – CENÁRIOS DE TESTES REALIZADOS

Este apêndice apresenta as cópias de tela que mostram os passos realizados nos cenários de testes do capítulo 6.

### Capturas de Tela dos Testes Realizados no Cenário 1

#### RDM aberta com sucesso no CRM Dynamics

The screenshot shows the Microsoft Dynamics CRM interface for 'Gestão de Mudança'. The main area displays a change request record titled 'SC-831887 - Teste cenário 1' under the 'Geral' tab. The record details include:

- Id da Mudança:** RDM-0013486
- Situação:** Nova
- Data de Criação:** 17/06/2015, 23:29
- Proprietário:** Luiz Fernando Portella
- Solicitante:** Leonardo Paim Magalhães
- Mudança:** SC-831887 - Teste cenário 1
- Descrição do Problema:** Teste cenário 1

The left sidebar shows navigation links for 'Informações' (Geral, Implementação, Anotações) and 'Relacionadas' (Comum: Atividades, Atividades Fechadas, Histórico de Auditoria, Ocorrências, Gestão de Demandas, Apontamento de Horas, Registros de Problema).

#### Tarefa de aprovação gerada automaticamente com sucesso

The screenshot shows the Microsoft Dynamics CRM interface for 'Atividades' (Activities). The main area displays a list of activities for the change request 'SC-831887 - Teste cenário 1'. One activity is listed:

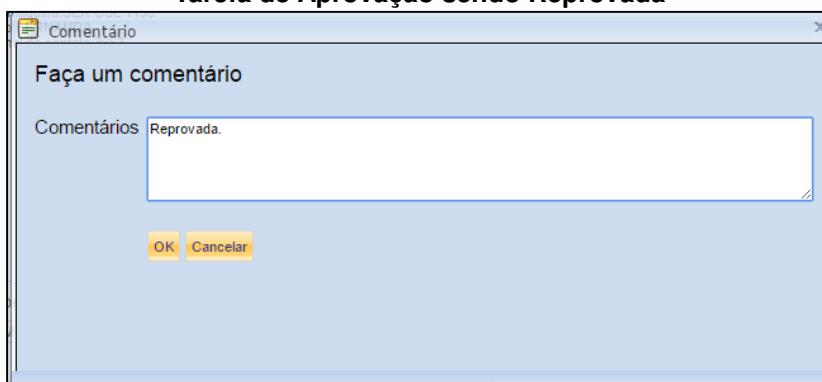
Assunto	Tipo de Atividade	Status da Ativida...	Prioridade
Aprovação Pendente de Gestão de Mudança	Tarefa	Aberta	Normal

The left sidebar shows navigation links for 'Informações' (Geral, Implementação, Anotações) and 'Relacionadas' (Comum: Atividades, Atividades Fechadas, Histórico de Auditoria, Ocorrências, Gestão de Demandas, Apontamento de Horas, Registros de Problema), as well as 'Processos' (Fluxos de Trabalho, Sessões de Diálogo).

### Tarefa de aprovação disponibilizada automaticamente no Portal de Serviços

The screenshot shows the CPFL Energia Service Portal interface. At the top, there's a navigation bar with links like 'Inicial', 'Meus Chamados', 'Infraestrutura Administrativa', 'Recursos Humanos', 'Suprimentos', 'Tecnologia da Informação', 'Financeiro, Contábil e Fiscal', 'Demandas', 'Aprovações', and 'Ajuda'. Below the navigation bar, a section titled 'Aprovações Pendentes' (Pending Approvals) is displayed. It includes a sub-section 'Lista' (List) with tabs 'Informações' and 'Ocorrências com Solução Proposta'. A table lists a single item: 'Mudança' (Change) with ID 'RDM-0013486', subject 'SIS - SAP/CCS - WF - Tabela de', status 'Aprovação' (Approval), creation date '17/06/2015 23:29', and responsible person 'Leonardo Paim Magalhães'. The table has columns: Entidade, Número, Assunto, Tarefa/Aprovação, Data de Criação, and Responsável.

### Tarefa de Aprovação sendo Reprovada



### RDM encerrada automaticamente como Reprovada

The screenshot shows the Microsoft Dynamics CRM interface for a 'Gestão de Mudança' (Change Management) record. The record ID is 'SC-831887 - Teste cenário 1'. The 'Informações' (Information) tab is selected, showing basic details: 'Id da Mudança' (Change ID) 'RDM-0013486', 'Situação' (Status) 'Reprovada' (Rejected), 'Data de Criação' (Creation Date) '17/06/2015 23:29', 'Proprietário' (Owner) 'Luiz Fernando Portela', 'Solicitante' (Requester) 'Leonardo Paim Magalhães', 'Grupo de Suporte' (Support Group) 'TI\_SAPCCS\_Basis', 'Mudança' (Change) 'SC-831887 - Teste cenário 1', 'Descrição do Problema' (Problem Description) 'Teste cenário 1', 'Descrição da Solução' (Solution Description) 'Teste cenário 1', and 'Status' (Status) 'Inativo(a)' (Inactive). The left sidebar shows related entities like 'Atividades', 'Histórico de Auditoria', 'Ocorrências', 'Gestão de Demandas', 'Apontamento de Horas', and 'Registros de Problema'.

## Capturas de Tela dos Testes Realizados no Cenário 2

### RDM aberta com sucesso no CRM Dynamics

The screenshot shows the Microsoft Dynamics CRM interface for 'Gestão de Mudança'. The main area displays a record titled 'SC-831887 - Teste cenário 2' with the status 'Nova' (New). The 'Informações' section includes fields for 'Id da Mudança' (RDM-0013487), 'Situção\*' (Status\*), 'Data de Criação' (Creation Date: 18/06/2015, 00:36), 'Proprietário\*' (Owner: Luiz Fernando Portella), 'Solicitante\*' (Requester: Leonardo Paim Magalhães), 'Mudança\*' (Change: SC-831887 - Teste cenário 2), and 'Descrição do Problema\*' (Problem Description: Teste cenário 2).

### RDM sinalizada com Cancelada no CRM Dynamics

This screenshot shows the same RDM record from the previous screen, but with different status settings. The 'Implementado com Sucesso?' (Implemented with Success?) field has 'Não' (No) selected. The 'Cancela RDM' (Cancels RDM) field has 'Sim' (Yes) selected. The 'Motivo de Cancelamento' (Reason for Cancellation) field contains the text 'Cancelada conforme teste cenário 2' (Cancelled according to scenario test 2).

### RDM encerrada como Cancelada no CRM Dynamics

The final screenshot shows the RDM record with all fields filled in, including the 'Situação\*' (Status\*) field set to 'Cancelada' (Cancelled). The 'Descrição da Solução\*' (Solution Description) field also contains the text 'Teste cenário 2'.

## Capturas de Tela dos Testes Realizados no Cenário 3

### RDM aberta com sucesso no CRM Dynamics

The screenshot shows the Microsoft Dynamics CRM interface for a 'Gestão de Mudança' (Change Management) record. The record ID is SC-831887 - Teste cenário 3. The 'Informações' (Information) section is expanded, showing the following details:

- Geral:**
  - Id da Mudança: RDM-0013488
  - Situação\*: Nova
  - Data de Criação: 18/06/2015, 01:17
  - Proprietário\*: Luiz Fernando Portella
  - Solicitante\*: Leonardo Paim Magalhães
  - Grupo de Suporte\*: TI\_CPF\_Energia\_Basis
  - Mudança\*: SC-831887 - Teste cenário 3
  - Descrição do Problema\*: Teste cenário 3

### RDM aprovada e passada para Em Atendimento

The screenshot shows the Microsoft Dynamics CRM interface for the same 'Gestão de Mudança' record. The 'Informações' section is expanded, showing the following details:

- Geral:**
  - Id da Mudança: RDM-0013488
  - Situação\*: Em Atendimento
  - Data de Criação: 18/06/2015, 01:17
  - Proprietário\*: Luiz Fernando Portella
  - Solicitante\*: Leonardo Paim Magalhães
  - Grupo de Suporte\*: TI\_CPF\_Energia\_Basis
  - Mudança\*: SC-831887 - Teste cenário 3
  - Descrição do Problema\*: Teste cenário 3

### RDM sinalizada para finalizar sem ser atendida com sucesso

The screenshot shows the Microsoft Dynamics CRM interface for the same 'Gestão de Mudança' record. The 'Informações' section is expanded, showing the following details:

- Número e Descrição da Request\***: Teste cenário 3
- Implementado com Sucesso?**: Não
- Finaliza RDM?**: Sim
- Data Real de Implementação\***: 18/06/2015
- Implementado Por\***: Leonardo Paim Magalhães
- Cancela RDM?**: Não
- Anotações** section contains: Status Ativo(a)

### RDM encerrada como Não Atendida no CRM Dynamics

The screenshot shows the Microsoft Dynamics CRM interface for 'Gestão de Mudança'. The main window displays a record for 'SC-831887 - Teste cenário 3'. The 'Informações' section is expanded, showing the 'Geral' tab selected. The 'Situção' field is set to 'Não Atendida'. Other fields include 'Data de Criação' (18/06/2015), 'Proprietário' (Luiz Fernando Portella), 'Solicitante' (Leonardo Paim Magalhães), 'Mudança' (SC-831887 - Teste cenário 3), and 'Descrição do Problema' (Teste cenário 3). The 'Relacionadas' sidebar lists various related entities like Activities, Closed Activities, Audit History, Occurrences, and Demand Management.

### Capturas de Tela dos Testes Realizados no Cenário 4

#### RDM aberta com sucesso no CRM Dynamics

The screenshot shows the Microsoft Dynamics CRM interface for 'Gestão de Mudança'. The main window displays a record for 'SC-831887 - Teste cenário 4'. The 'Informações' section is expanded, showing the 'Geral' tab selected. The 'Situção' field is set to 'Nova'. Other fields include 'Data de Criação' (18/06/2015), 'Proprietário' (Leonardo Paim Magalhães), 'Solicitante' (Leonardo Paim Magalhães), 'Mudança' (SC-831887 - Teste cenário 4), and 'Descrição do Problema' (Teste cenário 4). The 'Relacionadas' sidebar lists various related entities like Activities, Closed Activities, Audit History, Occurrences, and Demand Management.

#### RDM sinalizada para finalizar sendo atendida com sucesso

The screenshot shows the Microsoft Dynamics CRM interface for 'Gestão de Mudança'. The main window displays a record for 'SC-831887 - Teste cenário 4'. The 'Informações' section is expanded, showing the 'Implementação' tab selected. The 'Número e Descrição da Request' field contains 'Teste cenário 4 - Atendida'. Below it, the 'Implementado com Sucesso?' field has 'Sim' selected. The 'Finaliza RDM?' field has 'Sim' selected. The 'Data Real de Implementação' field shows '18/06/2015'. The 'Implementado Por' field shows 'Leonardo Paim Magalhães'. The 'Relacionadas' sidebar lists various related entities like Activities, Closed Activities, Audit History, Occurrences, and Demand Management.

**RDM encerrada como Atendida no CRM Dynamics**

The screenshot shows the Microsoft Dynamics CRM interface for a 'Gestão de Mudança' (Change Management) record. The record ID is SC-831887 - Teste cenário 4. The 'General' section displays basic information: Id da Mudança (RDM-0013489), Situação (Atendida), Data de Criação (18/06/2015, 01:56), Proprietário (Leonardo Paim Magalhães), Solicitante (Leonardo Paim Magalhães), Grupo de Suporte (TI\_SAPCCS\_Basis), Mudança (SC-831887 - Teste cenário 4), and Descrição do Problema (Teste cenário 4). The 'Status' field shows 'Inativo(a)'. The left sidebar lists related entities like Atividades, Ocorrências, and Gestão de Demandas. The top navigation bar includes options like Salvar e Novo, Compartilhando, Atribuir, Executar Fluxo de Trabalho, Iniciar Diálogo, and Executar Relatório.