UNIVERSIDADE DO VALE DO RIO DOS SINOS – UNISINOS
UNIDADE ACADÊMICA DE EDUCAÇÃO CONTINUADA
MBA EM ADMINISTRAÇÃO DA TECNOLOGIA DA INFORMAÇÃO

JEAN MICHEL FUCHS

ALINHAMENTO ENTRE COBIT E ISO 27005:2008 NA GESTÃO DE RISCOS DE TI

SÃO LEOPOLDO
2010

Jean Michel Fuchs

ALINHAMENTO ENTRE COBIT E ISO 27005:2008 NA GESTÃO DE RISCOS DE TI

Trabalho de Conclusão de Curso de Especialização apresentado como requisito parcial para a obtenção de título de Especialista em Administração da Tecnologia da Informação, pelo MBA Administração de TI da Universidade do Vale do Rio dos Sinos.

Orientador: Prof. ME. Henrique Jorge Brodbeck

São Leopoldo
2010

Jean Michel Fuchs

ALINHAMENTO ENTRE COBIT E ISO 27005:2008 NA GESTÃO DE RISCOS DE TI

Trabalho de Conclusão de Curso de Especialização apresentado como requisito parcial para a obtenção de título de Especialista em Administração da Tecnologia da Informação, pelo MBA Administração de TI da Universidade do Vale do Rio dos Sinos.

Aprovado em:

BANCA EXAMINADORA

Componente da Banca Examinadora – UNISINOS

Componente da Banca Examinadora – UNISINOS

Componente da Banca Examinadora – UNISINOS

AGRADECIMENTOS

Agradeço muito a Deus que me concedeu inspiração e momentos de força em toda minha vida. Tenho certeza que caminha ao meu lado.

A meus pais Erich e Vera, exemplos dedicação, humildade, sabedoria e amor à família. É inestimável a importância de ambos para o meu desenvolvimento.

A toda a minha família que sempre unida torna harmoniosa e prazerosa a vida.

À minha namorada, sempre paciente e compreensiva com os momentos ausentes e com outros de somente corpo presente, dedicando incontáveis cuidados e força sempre que necessário.

Ao meu orientador Henrique Jorge Brodbeck pelo seu vasto conhecimento compartilhado e dedicação para o desenvolvimento deste trabalho.

A meus colegas de trabalho e amigos pela disposição em ajudar sempre que possível.

A todos que de alguma forma ajudam no meu desenvolvimento profissional e pessoal.

RESUMO

A Gestão de Riscos (GR) de Segurança da Informação (SI) nos dias atuais tornou-se imprescindível para as organizações, sendo que em muitas vezes é impulsionada pela necessidade de conformidade com leis, regulamentações, padrões ou normas. Diante do desafio de implementar uma GR de SI efetiva, gestores acabam desenvolvendo ações sem uma estrutura ou metodologia de trabalho definida, consequentemente o objetivo esperado não é atingido, gerando retrabalho e custo para a empresa. O objetivo do presente trabalho foi elaborar um modelo estruturado em etapas para a implementação de GR de SI alinhado ao processo PO09 “Avaliar e Gerenciar os Riscos de TI” do CobiT 4.1 e a norma NBR ISO/IEC 27005:2008, definindo assim uma ordem para a implementação com as principais ações a serem executadas. Com este modelo estruturado, fica evidente que a utilização de somente uma norma ou um *framework* não é suficiente, sendo necessária a complementaridade de mais de uma norma ou *framework*, ampliando assim a abrangência da GR de SI assegurando a sua efetividade.

Palavras-chave: Gestão de Riscos. CobiT 4.1. NBR ISO/IEC 27005:2008. Segurança da Informação.

ABSTRACT

Nowadays Risk Management (RM) in Information Security (IS) has become indispensable for business organizations and it has been triggered several times by the necessity of acting in response to laws, regulations, standards or norms. When facing the challenge to implement RM in effective SI, managers end up developing actions without delineating any structure or work methodology. Therefore the expected objective is not reached what generates redoing and costs for the company. The objective of the work presented here is to elaborate a structured model in stages to implement RM for IS which is aligned to PO09 process “Assess and Manage IT Risks” from CobiT 4.1 and regulations from NBR ISO/IEC 27005:2008 thus defining an order for the implementation of the main actions to be executed. Through this structured model, it gets evident that the usage of only one norm or framework is not enough; being necessary a complement of one or more norms or framework to expand the scope of RM in IS in order to assure its effectiveness.

Keywords: Risk Management. CobiT 4.1. ISO/IEC 27005:2008. Information Security.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
CIO	*Chief Information Officer*
COBIT	*Control Objectives for Information and related Technology*
GR	Gestão de Riscos
ISO	*International Organization for Standardization*
ITIL	*Information Technology Infrastructure Library*
SGSI	Sistema de Gestão de Segurança da Informação
SI	Segurança da Informação
TI	Tecnologia da Informação
PDCA	*Plan – Do – Check – Act*
ISACF	*Information Systems Audit and Control Foundation*

SUMÁRIO

1 INTRODUÇÃO

Atualmente as empresas de todo o mundo dependem de informações para tomada de decisões e sustentação das operações do negócio. Neste cenário percebe-se um crescimento da necessidade de gerenciar os riscos que cercam estas informações, mantendo-as disponíveis com integridade e total confidencialidade. Segundo a 10ª Pesquisa Nacional Sobre Segurança da Informação (MÓDULO *SECURITY*,2007) 65% das empresas pesquisadas não tem uma metodologia formalizada para análise de riscos em Tecnologia da Informação (TI), sendo que 22% destas nunca realizaram uma análise de riscos na área de TI.

Diante da necessidade de mitigar o grande número de ameaças existentes, os riscos devem ser identificados, analisados, avaliados e tratados, sendo que o objetivo final do processo é que o risco seja reduzido ao nível aceitável, levando em consideração que o custo para o seu tratamento não deve ultrapassar os prejuízos causados pelo risco (SALES, 2010).

Todas as organizações, de qualquer porte, estão vulneráveis a ameaças de segurança da informação, que ameaça podem simplesmente causar uma indisponibilidade em um serviço pouco crítico como também podem gerar vazamento de informações, comprometendo assim a imagem e a reputação da empresa.

1.1 TEMA E CONTEXTUALIZAÇÃO DO PROBLEMA

O tema deste trabalho é Gestão de Riscos (GR) de TI com foco na norma ABNT NBR ISO/IEC 27005 (ABNT, 2008) e no processo “Avaliar e Gerenciar os Riscos de TI” do *Control Objectives for Information and related Technology* (COBIT® 4.1) (ITGI, 2007).

1.2 PROBLEMA DE PESQUISA

Com o aumento constante de ameaças aos ativos das empresas, inúmeras leis, regulamentações e normas entraram em vigor para impor às organizações de vários ramos de atividades inúmeras regras e padrões no que tange a segurança da informação. Dentre estas regras uma delas é a necessidade de efetuar a gestão dos riscos relacionados a estes ativos, iniciando neste momento as dúvidas de muitos gestores de TI na decisão de como iniciar o processo de implementação de uma GR de SI.

Dentro do contexto atual onde a área de TI necessita do alinhamento estratégico com o negócio da empresa, vários *frameworks* de Governança de TI surgem no mercado, sendo eles em alguns momentos superficiais no que tange ao gerenciamento de riscos dos ativos do negócio. Segundo Heiser (2009), os profissionais da Segurança da Informação cometem quatro erros comuns na GR sendo eles descritos abaixo:

- Assumir uma abordagem do tipo *"One Size Fits All"* (uma solução padrão para todos) para a gestão da segurança e dos riscos.
- Fazer planos com base naquilo que a organização de segurança quer, e não no que a empresa precisa.
- Fazer com que as comunicações relativas aos riscos sejam complexas demais para que a empresa compreenda.
- Permitir que os gerentes de linha dos negócios transfiram seus riscos para a organização de TI e para a organização de segurança de TI.

Em vários momentos gestores de TI executam ações isoladas para a mitigação de riscos sem nenhuma metodologia estruturada, gerando muitas vezes uma falsa sensação de segurança.

Com base nestas informações e na necessidade de implantação de uma GR de SI mais eficiente, quais os requisitos e etapas necessárias para um alinhamento entre o *framework* de governança CobiT e a norma NBR ISO 27005 (ABNT, 2008) para a GR de SI?

1.3 OBJETIVOS

1.3.1 Objetivo Geral

Os objetivos deste trabalho são identificar e elaborar um modelo estruturado de para a implementação de uma GR de SI, com base na norma NBR ISO 27005 (ABNT, 2008) e no *framework* de governança CobiT, sendo este modelo direcionado para organizações de médio a grande porte com uma área de Tecnologia da Informação definida e estruturada.

1.3.2 Objetivos Específicos

Os objetivos específicos deste trabalho são os citados abaixo:

- Identificar as definições sobre Segurança da Informação e Gestão de Riscos da Tecnologia da Informação a partir de uma revisão bibliográfica.
- Descrever cada requisito da norma NBR ISO 27005 (ABNT, 2008).
- Descrever os objetivos e métricas propostos no P09 “Avaliar e Gerenciar os Riscos de TI” do CobiT.
- Efetuar o alinhamento entre o a norma NBR ISO 27005 (ABNT, 2008) e o processo PO9 “Avaliar e Gerenciar os Riscos de TI” do CobiT.
- Desenvolver um modelo estruturado em etapas para o controle da implantação da GR em conformidade com os requisitos da norma NBR ISO 27005 (ABNT, 2008) alinhados aos objetivos de controle do P09 “Avaliar e Gerenciar os Riscos de TI” do CobiT.

1.4 JUSTIFICATIVA

Com a grande utilização dos recursos de informática, identifica-se uma grande dificuldade dos CIO’s na aprovação de projetos referentes à Segurança da Informação. A 10ª Pesquisa Nacional Sobre Segurança da Informação (MÓDULO *SECURITY*, 2007), identificou-se que 55% das empresas informaram que o principal obstáculo para a implementação da Segurança da Informação foi a falta de

conscientização dos executivos e usuários. Conforme a norma ABNT NBR ISO/IEC 27001 (ABNT, 2006) versa,

> A organização deve estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um SGSI documentado dentro do contexto das atividades de negócio globais da organização e os riscos que ela enfrenta.

A GR se faz um processo necessário e essencial para um SGSI (Sistema de Gestão de Segurança da Informação) consistente e efetivo, visto que diariamente surgem novas ameaças que exploram vulnerabilidades nos ativos do negócio, causando em vários momentos indisponibilidades, vazamento de informações, perdas financeiras e até mesmo uma degradação da imagem da empresa perante o mercado.

Outro fator importante na implantação de uma GR é a conformidade com legislações vigentes para alguns setores, principalmente bancos, entidades financeiras, empresas do setor de saúde, telefônicas, dentre outras.

Em face do desafio de formular e iniciar a GR de SI o presente trabalho pretende auxiliar gestores de Segurança da Informação no desenvolvimento de uma política de GR, norteando-os dos principais requisitos necessários que devem ser aplicados com base na norma NBR ISO 27005 (ABNT, 2008) e no CobiT 4.1, sendo eles descritos na forma de um modelo estruturado por etapas em uma sequência definida para a implementação.

O presente trabalho está organizado da seguinte forma: o capítulo 2 apresenta conceitos básicos sobre gestão de riscos de segurança da informação, descrição das duas principais normas para gestão de riscos e o *framework* CobiT, o capítulo 3 aborda qual foi a metodologia utilizada para o desenvolvimento do estudo, o capítulo 4 descreve em detalhes a norma NBR ISO 27005 e o processo PO9 “Avaliar e Gerenciar os Riscos de TI” do CobiT 4.1, no capítulo 5 são apresentadas duas tabelas com o alinhamento entre a norma e o *framework* CobiT com foco em GR de SI, o capítulo 6 inclui o modelo estruturado para a GR de SI onde estão descritas as principais ações a serem executas separadas em etapas ordenadas e o capítulo 7 finaliza o presente trabalho com as conclusões e trabalhos futuros.

2 FUNDAMENTAÇÃO TEÓRICA

Este capítulo tem como objetivo esclarecer a teoria dos assuntos tratados neste estudo, contextualizando o que é um Sistema de Gestão de Segurança da Informação, Sistema de Gestão de Riscos da Segurança da Informação, o *framework* CobiT, bem com as normas NBR ISO 27005 e ISO/IEC 31000:2009 *General guidelines for principles and implementation of risk management.*

2.1 Sistema de Gestão de Segurança da Informação

De acordo com a norma NBR ISO 27005 (ABNT, 2005) “A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e consequentemente necessita ser adequadamente protegida.” Esta afirmação é reforçada com a grande dependência das empresas de seus sistemas informatizados, pois atualmente o maior valor do negócio são as suas informações, parte do seu capital intangível.

Segundo Sêmola (2003) a definição de informação é descrita conforme abaixo:

> Conjunto de dados utilizados para a transferência de uma mensagem entre indivíduos e/ou máquinas em processos comunicativos (isto é, baseados em troca de mensagens) ou transacionais (isto é, processos em que sejam realizadas as operações que envolvam, por exemplo, a transferência de valores monetários).

A segurança da informação tem como norteadores os três princípios básicos, sendo eles descritos abaixo:

- **Confidencialidade:** toda a informação deve ser mantida em sigilo e com garantia de que somente será acessada pelas pessoas que tenham direito para tal.
- **Disponibilidade:** toda a informação deve estar disponível para seus usuários autorizados sempre que os mesmos solicitarem.

- **Integridade:** a informação deve estar protegida e isenta de erros, sendo mantida da forma que foi criada pelo seu autor.

Segundo a NBR ISO 27001 (ABNT, 2006), um Sistema de Gestão de Segurança da Informação é representado conforme a figura 1:

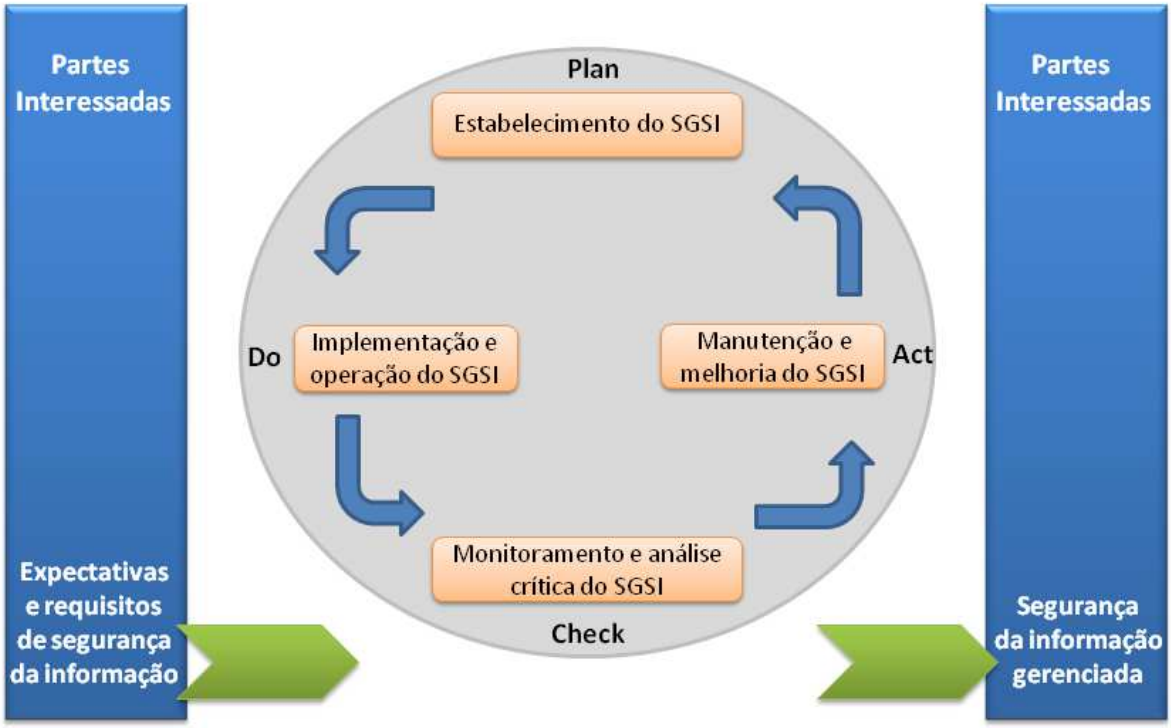

Figura 1 – Modelo PDCA aplicado aos processos do SGSI.
Fonte: NBR ISO 27001 (ABNT, 2006).

Com base na figura 1, a norma NBR ISO 27001 (ABNT, 2006) descreve cada etapa conforme abaixo:

- ***Plan* (planejar):** Estabelecer a política, objetivos, processos e procedimentos do SGSI, relevantes para a gestão de riscos e a melhoria da segurança da informação para produzir resultados de acordo com as políticas e objetivos globais de uma organização.
- ***Do* (fazer):** Implementar e operar a política, controles, processos e procedimentos do SGSI.
- ***Check* (checar):** Avaliar e, quando aplicável, medir o desempenho de um processo frente à política, objetivos e experiência prática do SGSI e apresentar os resultados para a análise crítica pela direção.

- ***Act* (agir):** Executar as ações corretivas e preventivas, com base nos resultados da auditoria interna do SGSI e da análise crítica pela direção ou outra informação pertinente, para alcançar a melhoria contínua do SGSI.

Conforme a figura 1, o processo inicia pelas partes interessadas, também conhecidas como *stakeholders*, sendo que a entrada para o SGSI são as expectativas e os requisitos das partes interessadas e ao final do processo a Segurança da Informação estará gerenciada.

Segundo a pesquisa TIC Empresas 2008 realizada pelo NIC.br (Núcleo de Informação e Coordenação do Ponto BR), 63% das pequenas e médias empresas brasileiras podem deixar de existir ou sofrer um prejuízo de ordem financeira que poderia inviabilizar a continuidade dos negócios em função de vulnerabilidades, sejam elas naturais ou ameaças virtuais pela falta da definição de um SGSI.

Em virtude da grande dificuldade no desenvolvimento de um SGSI a norma ABNT NBR ISO/IEC 27002 (ABNT, 2005) prescreve dez fatores críticos de sucesso na implementação de um SGSI, sendo eles listados abaixo:

- Política de segurança da informação, objetivos e atividades, que reflitam os objetivos do negócio.
- Uma abordagem e uma estrutura para a implementação, manutenção, monitoramento e melhoria da segurança da informação que seja consistente com a cultura organizacional.
- Comprometimento e apoio visível de todos os níveis gerenciais.
- Um bom entendimento dos requisitos de segurança da informação, da análise/avaliação de riscos e da gestão de riscos.
- Divulgação eficiente da segurança da informação para todos os gerentes, funcionários e outras partes envolvidas para se alcanças a conscientização.
- Distribuição de diretrizes e normas sobre a política de segurança da informação para todos os gerentes, funcionários e outras partes envolvidas.

- Provisão de recursos financeiros para as atividades da gestão de segurança da informação.
- Provisão de conscientização, treinamento e educação adequados.
- Estabelecimento de um eficiente processo de gestão de incidentes de segurança da informação.
- Implementação de um sistema de medição, que seja usado para avaliar o desempenho da gestão da segurança da informação e obtenção de sugestões para a melhoria.

2.2 Sistema de Gestão de Riscos da Segurança da Informação

No contexto de um SGSI, uma das etapas mais importantes é o Sistema de Gestão de Riscos da Segurança da Informação. Segundo a norma NBR ISO 27005 (ABNT, 2008), o processo de GR é descrito abaixo conforme figura 2:

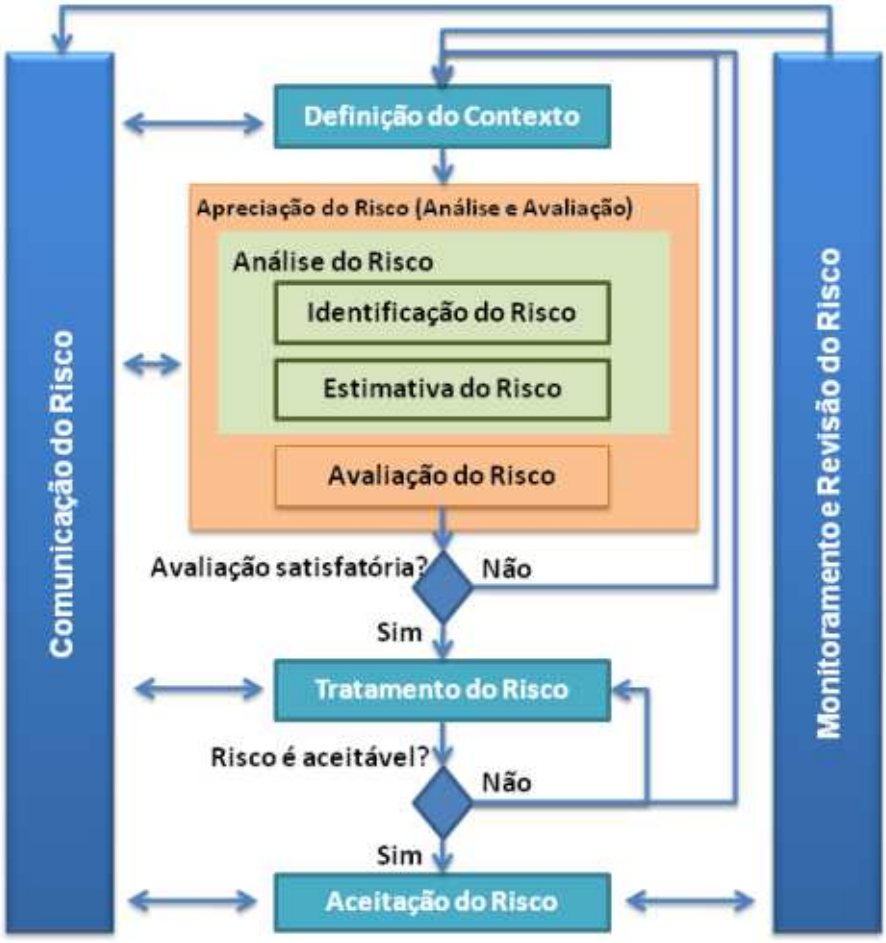

Figura 2 – Processo de Gestão de Riscos.

Fonte: NBR ISO 27005 (ABNT, 2008).

Segundo Sales (2010), a gestão de riscos pode ser definida conforme abaixo:

> "[..]é um processo sistemático para identificar, analisar, avaliar e tratar os riscos e permite melhorar o desempenho da organização por meio da identificação de oportunidades de ganhos e de redução de probabilidades ou impactos de perdas, indo além de demandas regulatórias. O processo de avaliação de riscos (*risk assessment*), na verdade, não é um processo único e, sim, uma composição de três outros processos: identificação de riscos, análise de riscos e avaliação de riscos. O objetivo final do processo é sempre que o risco seja reduzido ao nível aceitável, o que significa que o custo do tratamento não deve ultrapassar o custo proporcionado pelo risco.

Existem atualmente duas principais normas para Gestão de Riscos de Segurança da Informação, a primeira delas é a norma ABNT NBR ISO/IEC 27005 (ABNT, 2008) e a ISO/IEC 31000:2009.

2.2.1 A norma NBR ISO 27005:2008

Fornece diretrizes para o processo de Gestão de Riscos de Segurança da Informação levando em consideração os requisitos de um SGSI em conformidade com a NBR ISO 27001 (ABNT, 2006). O principal objetivo desta norma é orientar a implementação de um processo de gestão de riscos, sendo que ela não tem uma metodologia específica para a gestão de riscos de segurança da informação, cabendo à organização definir a sua abordagem para este assunto.

Esta norma é dividida nas seções abaixo:

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

Segundo a norma NBR ISO 27005 (ABNT, 2008), as seções descritas acima contribuem diretamente para:

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

O processo de SGSI está alinhado ao processo de gestão de riscos de segurança da informação conforme tabela 1.

Tabela 1 - Alinhamento do processo de SGSI e do processo de gestão de riscos de segurança da informação

Processo do SGSI	Processo de gestão de riscos de segurança da informação
Planejar	Definição do contexto Análise/avaliação de riscos Definição do plano de tratamento do risco Aceitação do risco
Executar	Implementação do plano de tratamento do risco
Verificar	Monitoramento contínuo e análise crítica de riscos
Agir	Manter e melhorar o processo de Gestão de Riscos de Segurança da Informação

Fonte: NBR ISO 27005 (ABNT, 2008).

2.2.2 A norma ISO/IEC 31000:2009

A norma ISO/IEC 31000:2009 é uma norma de gerenciamento de riscos que pode ser aplicada a qualquer tipo de risco, podendo também ser implementada em qualquer tipo de organização. O seu desenvolvimento derivou da norma AS/NZS 4360 em 2005. A norma ISO/IEC 31000:2009 foi traduzida para português e publicada em Novembro de 2009 sendo referenciada como ABNT NBR ISO/IEC 31000:2009 (ABNT, 2009).

A figura 3 ilustra o processo de gerenciamento de riscos descrito na norma ISO/IEC 31000:2009.

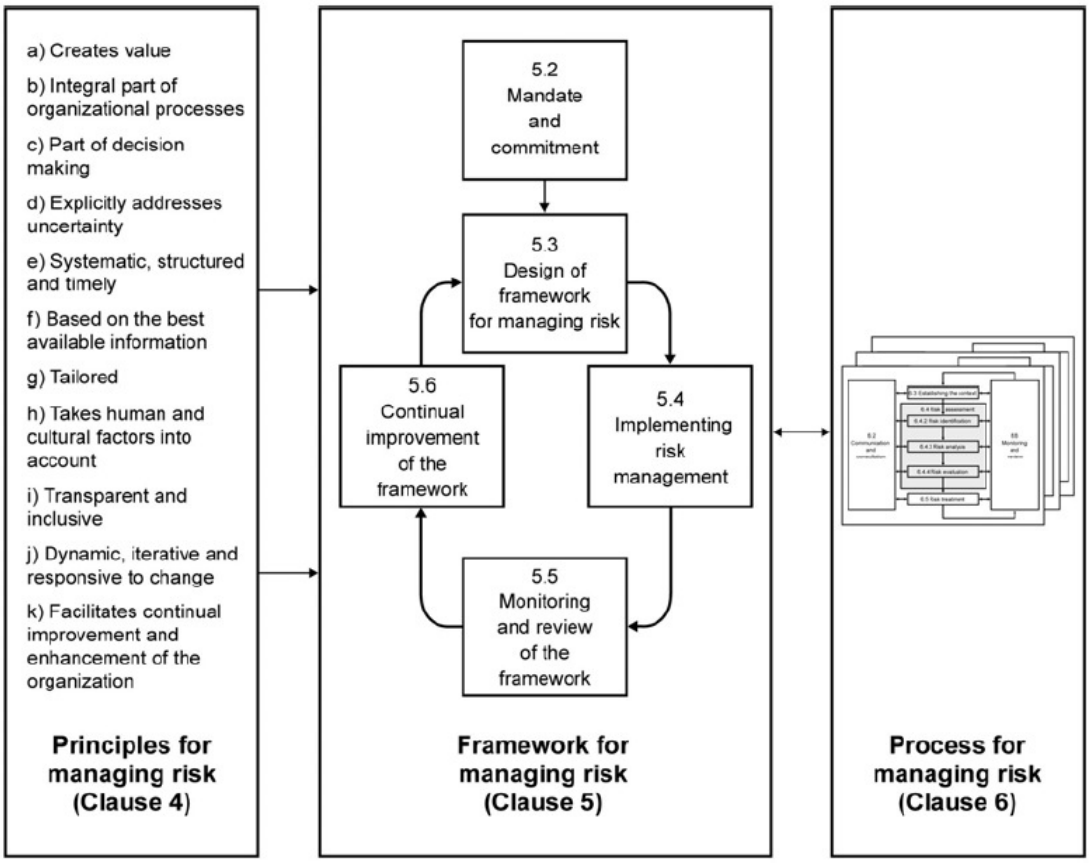

Figura 3 - Processo de Gestão de Riscos de acordo com norma ISO/IEC 31000:2009.
Fonte: ISO/IEC 31000:2009.

O processo de gestão de riscos da norma ISO/IEC 31000:2009 está dividido em três partes, sendo elas, Princípios para Gerenciamento do Risco, *Framework* para Gerenciamento do Risco e Processos para Gerenciamento do Risco.

Os princípios de gestão de riscos são os descritos abaixo, sendo que estes princípios são o resultado esperado de uma gestão de riscos eficiente:

- Criar valor.
- Ser parte integral dos processos organizacionais.
- Ser parte da tomada de decisão.
- Endereçar a incerteza explicitamente.
- Ser sistemática, estruturada e oportuna.
- Ser baseado na melhor informação possível.
- Ser customizado.
- Levar em conta fatores humanos e culturais.
- Ser transparente e inclusivo.
- Ser dinâmico, iterativo e responder às mudanças.
- Facilitar a melhoria contínua.

Todos os processos para GR de acordo com a norma NBR ISO 27005 (ABNT, 2008), serão discutidos em detalhes no capítulo quatro do presente trabalho.

2.3 Conceitos de Gestão Riscos da Segurança da Informação

Alguns conceitos no processo de Gestão de Riscos da Segurança da Informação divergem de uma norma para a outra. Por este motivo, abaixo serão contextualizados os principais conceitos utilizado neste trabalho de acordo com as normas NBR ISO 27001, NBR ISO 27002, NBR ISO 27005 e NBR ISO 31000.

2.3.1 Ameaças

As ameaças tem o poder de comprometer os ativos de uma organização, causando assim um impacto que pode ocasionar em perdas para a organização.

De acordo com a norma NBR ISO 27005 (ABNT, 2008), as ameaças são descritas conforme a figura 4.

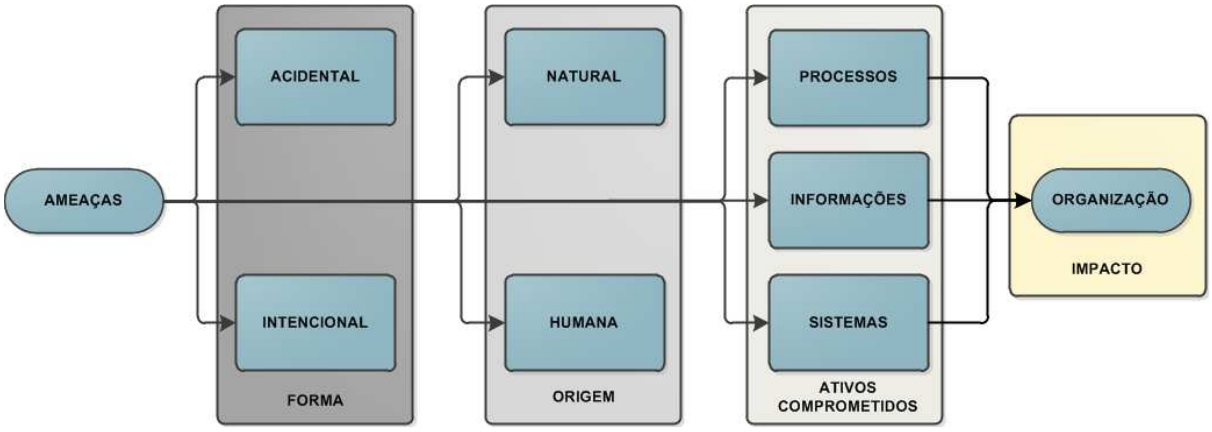

Figura 4 - Fluxo de ameaças.

Fonte: Criação própria através de interpretação da norma NBR ISO 27005 (ABNT, 2008).

Conforme ilustrado na figura 4, as ameaças podem ocorrer de duas formas, acidental ou intencional, sendo que quando a origem da ameaça for natural, ela nunca será intencional. As origens possíveis de uma ameaça são naturais e humanas. Toda a ameaça compromete um ou mais ativos, sendo que eles foram divididos em três grandes grupos como processos, informações e sistemas que por consequência toda a ameaça gera um impacto, neste caso, a organização.

Na tabela 2 são exemplificadas algumas ameaças relacionadas ao seu tipo e origem de acordo com a norma NBR ISO 27005 (ABNT, 2008).

Tabela 2 - Exemplos de ameaças descritas na norma NBR ISO 27005 (ABNT, 2008).

Tipo	Ameaças	Origem
Dano físico	Poeira, corrosão, congelamento.	Acidental, Intencional, Natural.
Eventos naturais	Inundação	Natural
Paralisação de serviços essenciais	Interrupção do fornecimento de energia	Acidental, Intencional, Natural.
Comprometimento da informação	Furto de mídia ou documentos	Intencional
Falhas técnicas	Defeito de equipamento	Acidental
Ações não autorizadas	Processamento ilegal de dados	Intencional
Comprometimento de funções	Abuso de direitos	Acidental, Intencional

Fonte: NBR ISO 27005 (ABNT, 2008).

2.3.2 Ativos

Ativo é tudo que tem valor para a organização e que deve ser protegido. Dentro do escopo de uma GR todos os ativos devem ser identificados, sendo que de acordo com a norma NBR ISO 27005, dois tipos de ativos podem ser diferenciados:

- **Ativos primários:**
  - Processos e atividades do negócio
  - Informações
- **Ativos de suporte e infraestrutura:**
  - Hardware
  - Software
  - Rede
  - Recursos humanos
  - Instalações físicas
  - A estrutura da organização

Um processo muito importante da GR é a valoração dos ativos que compreende em classificar os ativos conforme o seu valor para a organização. Para alguns ativos é possível utilizar uma valoração monetária sendo possível ainda, utilizar uma avaliação qualitativa para os demais ativos, utilizando algumas expressões como: pequeno, médio, alto.

2.3.3 Eventos

Conforme a norma ISO/IEC 31000:2009, evento é a ocorrência ou alteração de um determinado conjunto de circunstâncias.

2.3.4 Impacto

Impacto de acordo com a norma NBR ISO 27005 é o resultado causado por um incidente de segurança da informação. Este impacto está relacionado à medida do sucesso do evento de segurança da informação. O impacto de um evento

relacionado à segurança da informação deve ter critérios definidos para a sua classificação, alguns deles são:

- Dano à reputação
- Operações comprometidas (internas ou de terceiros)
- Interrupção de planos e o não cumprimento de prazos.

Para a avaliação do impacto, a norma NBR ISO 27005 considera que o impacto tem dois efeitos, um efeito imediato (operacional) ou uma consequência futura (relativa ao negócio como um todo), sendo que o efeito imediato pode ser direto ou indireto. Abaixo alguns exemplos de efeitos imediatos diretos e indiretos:

- **Direto:**
  - O valor financeiro de reposição do ativo perdido (ou parte dele).
  - Consequências resultantes de violações da segurança da informação.
- **Indireto:**
  - O custo das operações interrompidas.
  - Violação dos códigos éticos de conduta.

2.3.5 Incidente

Incidente segundo a norma NBR ISO 27002 pode ser definido como:

> Incidente de segurança da informação é indicado por um simples ou por uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação.

2.3.6 Risco

Segundo a norma NBR ISO 27005, risco é a combinação das consequências advindas da ocorrência de um evento indesejado e da probabilidade da ocorrência do mesmo. Risco de acordo com a norma ISO/IEC 31000:2009 é o efeito da incerteza sobre os objetivos.

Na figura 5 é descrito o fluxo do risco contendo os itens de ameaça, vulnerabilidade, ativo e impacto:

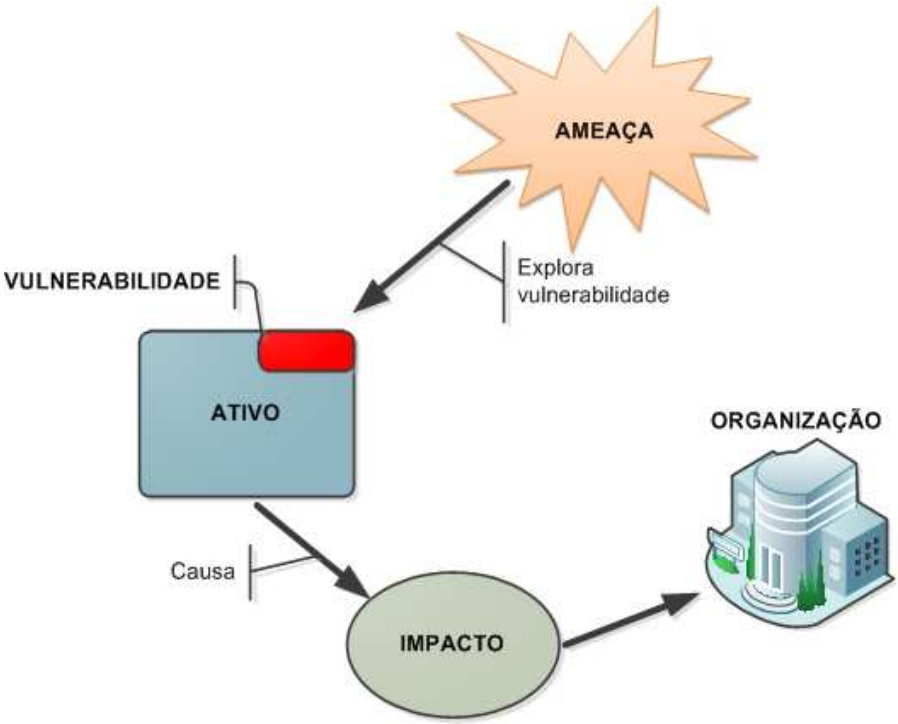

Figura 5 - Fluxo de risco.

Fonte: O autor, com base na norma NBR ISO 27005 (ABNT, 2008).

2.3.7 Vulnerabilidade

Vulnerabilidades de acordo com a norma NBR ISO 27002 é a fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

Uma vulnerabilidade pode não ser um problema se não houve nenhuma ameaça associada a ela, sendo que este fato não exclui a necessidade de monitoramento e análise da vulnerabilidade.

2.4 O *framework* de governança COBIT

O CobiT *(Control Objectives for Information and Related Technology)* foi criado em 1996 pela ISACF *(Information Systems Audit and Control Foundation)*. Em 1998 foi lançada a 2ª versão, sendo constituída de documentação de alto nível, controles, objetivos detalhados e criação do *Implementation Tool Set*. A 3ª edição

lançada em 2000 utilizou como foco principal a Governança de TI, sendo que em 2005 a 4ª e atual edição trouxe adequações necessárias para uma melhor integração com regulamentações como Basiléia e Sarbanes-Oxley.

O CobiT é dividido em quatro domínios conforme figura 6:

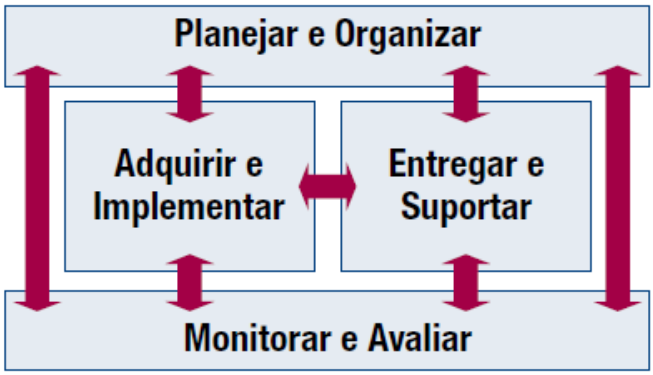

Figura 6 - Os Quatro Domínios Inter-relacionados do CobiT.
Fonte: CobiT (2007).

Segundo CobiT, os domínios demonstrados na figura 6 são denominados:

- **Planejar e Organizar (PO):** Provê direção para entrega de soluções (AI) e entrega de serviços (DS).
- **Adquirir e Implementar (AI):** Provê as soluções e as transfere para tornarem-se serviços.
- **Entregar e Suportar (DS):** Recebe as soluções e as torna passíveis de uso pelos usuários finais.
- **Monitorar e Avaliar (ME)**: Monitora todos os processos para garantir que a direção definida seja seguida.

Nestes domínios existem definidos 34 processos de controle de alto nível e 318 objetivos de controle.

Para atestar a maturidade de cada processo o CobiT utiliza um modelo de maturidade genérico com uma escala de seis estágios, sendo eles descritos abaixo:

- **Nível 0 – Inexistente:** Total falta de um processo reconhecido. A organização ainda não tem conhecimento que existe uma questão a ser trabalhada.

- **Nível 1 – Inicial / *Ad hoc*:** A organização evidencia que reconheceu existem questões a serem trabalhadas, porém ainda não existe um processo padronizado. Ao invés disto, existem métodos *ad hoc* que tendem a serem aplicados individualmente caso-a-caso. A sistemática geral de gerenciamento é desorganizada.
- **Nível 2 – Repetível e intuitivo:** Procedimentos similares são efetuados por pessoas diferentes fazendo a mesma tarefa. Não existe comunicação ou treinamento do processo, o que consequentemente fica atrelado ao conhecimento das pessoas envolvidas, o que pode acabar incorrendo em erros.
- **Nível 3 – Processos definidos:** Os procedimentos da organização foram padronizados, documentados e comunicados através de um treinamento. É obrigatório que estes procedimentos sejam seguidos mas como os procedimentos não são sofisticados, possíveis desvios não serão detectados.
- **Nível 4 – Gerenciados:** Os processos já são possíveis de serem monitorados e medidos, com isso ações pode ser tomadas onde o processo não está funcionando de forma adequada. A melhoria contínua dos processos está presente e fornecem boas práticas, sendo que ferramentas e automação são utilizadas de forma ainda decentralizada e limitada.
- **Nível 5 – Processos otimizados:** Os processos foram otimizados utilizando melhores práticas, melhoria contínua e a modelagem da maturidade como outras organizações. A TI é capaz de prover ferramentas para aprimorar a qualidade e efetividade da organização, sendo utilizada para automatizar o fluxo de trabalho, gerando maior agilidade para a organização adaptar-se de forma rápida.

Estes estágios de maturidade são representados de forma gráfica conforme figura 7:

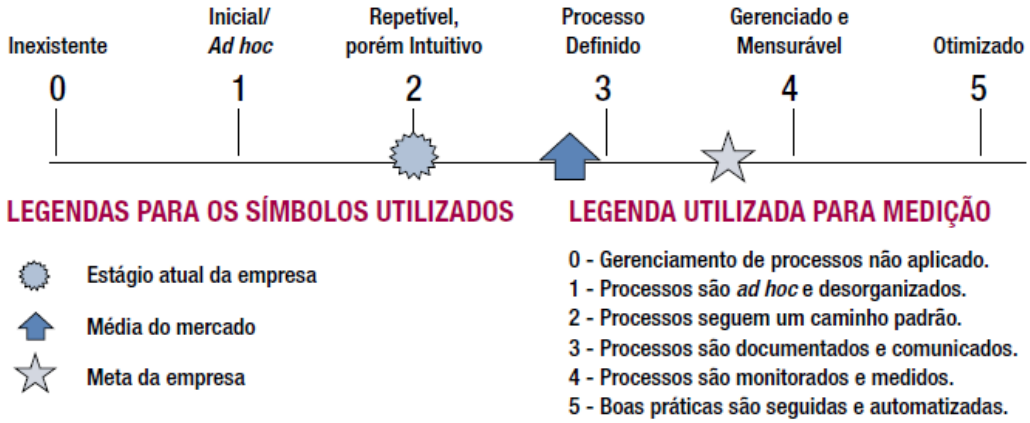

Figura 7 - Representação Gráfica dos Modelos de Maturidade.
Fonte: CobiT (2007).

Neste capítulo foram abordados conceitos de Sistema de Gestão de Segurança da Informação, Gestão de Riscos, as duas principais normas para gestão de riscos, além de elucidar a estrutura básica do *framework* CobiT.

No próximo capítulo será abordada a metodologia utilizada para o desenvolvimento do presente trabalho.

3 MÉTODO DE PESQUISA

Este capítulo aborda os métodos que apoiam e auxiliam para o desenvolvimento do estudo, bem como apresenta os demais procedimentos metodológicos utilizados.

O método do trabalho é constituído, segundo Leopardi (2001, p.295) pelo conjunto de recursos utilizados para alcançar os objetivos da pesquisa, ou seja, é o roteiro ou caminho que foi percorrido para execução, até a obtenção da resposta da questão/problema de investigação.

Cabe ressaltar que foram utilizados métodos para a Fundamentação Teórica, tais como a pesquisa bibliográfica, que para Vergara (2004), é de fundamental importância, pois fornece informações do tema ou assunto a ser estudado, bem como traz uma gama de linhas para escolha. Cabe então, escolher a linha de raciocínio que o pesquisador deseja seguir.

Roesch (2005, p.118) reforça também que o método escolhido tenha coerência com a formulação do problema, com os objetivos do projeto e com outras limitações (tempo, custo, disponibilidade de dados). Também expõe que “os métodos e técnicas oportunizam a exploração e a análise das situações problemáticas das organizações de forma mais aprofundada”.

3.1 DELINEAMENTO DA PESQUISA

Considerando os conceitos dos autores citados acima, para a realização deste estudo, que tem o intuito de confrontar os requisitos da norma NBR ISO 27005 com o *framework* de governança CobiT, para elaboração de um modelo estruturado nas etapas necessárias e essenciais para uma implementação de GR na área de TI, utilizou-se a pesquisa bibliográfica; pois esta é a base para elaboração de trabalhos científicos de qualquer natureza, sendo esgotada em si mesma, por se tratar de um trabalho teórico.

3.2 TÉCNICA DE COLETA DE DADOS

A coleta de dados, segundo Lakatos (2001), é a etapa de pesquisa em que se inicia a aplicação dos instrumentos elaborados e das técnicas selecionadas, a fim de efetuar a coleta de dados previstos.

É a fase prática da pesquisa, onde se inicia a aplicação do instrumento de coleta de dados e das técnicas selecionadas; é necessário um entrosamento das tarefas, cumprindo os prazos definidos e o orçamento previsto (Oliveira, 1998).

No presente trabalho a principal técnica de coleta de dados foi a pesquisa bibliográfica de publicações e normas estabelecidas, como o CobiT 4.1 e a NBR ISO 27005.

A decisão de escolha do *framework* CobiT 4.1 baseia-se na sua abrangência e visão de gerenciamento da área de TI. A escolha pela a norma NBR ISO 27005 justifica-se por ser uma das principais normas de gestão de riscos de TI atualmente, complementando as lacunas do CobiT 4.1.

Para a coleta de dados em ambos os documentos, CobiT 4.1 e norma NBR ISO 27005, foram analisados todos os requisitos, objetivos de controles, entradas/saídas e métricas existentes para a criação de um Modelo Estruturado para Gestão de Riscos de Segurança da Informação, sendo este modelo apresentado ao final do presente trabalho.

3.3 TÉCNICA DE ANÁLISE DE DADOS

Roesch (1996) determina na análise de dados que quando o pesquisador encerra a sua coleta, conta com uma quantidade imensa de anotações ou depoimentos, os quais se materializam na forma de textos; estes devem ser organizados para posterior interpretação.

“Os dados e as informações devem ser analisados visando à solução do problema de pesquisa proposto, o alcance dos objetivos colimados, bem como utilizados para se testar hipóteses enunciadas” (Martins, 2002, p.55).

Após a leitura da norma NBR ISO 27005, foram analisados todos os seus requisitos, identificando os seus pontos principais e ações necessárias para a implementação de cada requisito. Da mesma forma foi efetuado com o CobiT 4.1, após a leitura do processo PO9 “Avaliar e Gerenciar Riscos de TI” todos os objetivos de controles, saídas, entradas e métricas foram analisados, identificando as principais necessidades e ações a serem executadas.

Com o detalhamento das principais necessidades e ações a serem executadas, foram elaboradas duas tabelas de alinhamento sendo a primeira alinhando a norma NBR ISO 27005 com o PO9 “Avaliar e Gerenciar Riscos de TI” do CobiT 4.1 e após foi elaborado o alinhamento entre o processo PO9 “Avaliar e Gerenciar Riscos de TI” com a norma.

Identificando as lacunas existentes entre a norma NBR ISO 27005 e o CobiT 4.1, foi possível desenvolver um modelo estruturado nas principais etapas para a implementação de uma GR de SI com base nos requisitos identificados e analisados durante a coleta dos dados.

4 SISTEMA DE GESTÃO DE RISCOS DA SEGURANÇA DA INFORMAÇÃO COM COBIT 4.1 E NBR ISO 27005:2008

Neste capítulo serão abordadas todas as etapas necessárias para a Gestão de Riscos da Segurança da Informação conforme exigências da norma NBR ISO 27005:2008 e do processo P09 “Avaliar e Gerenciar os Riscos de TI” do CobiT 4.1.

4.1 Gestão de Riscos de Segurança da Informação com a norma NBR ISO 27005:2008

A norma NBR ISO 27005 é dividida em seis grandes etapas, sendo elas descritas abaixo:

- Definição de contexto
- Análise/avaliação de risco de segurança da informação
- Tratamento do risco de segurança da informação
- Aceitação do risco de segurança da informação
- Comunicação do risco de segurança da informação
- Monitoramento e análise crítica de riscos de segurança da informação

Cada etapa é composta por subetapas, sendo que cada uma delas será descrita ao longo deste capitulo.

4.1.1 Definição de contexto

Nesta etapa da norma, é necessário que a organização defina qual será o contexto do SGSI, contendo os critérios básicos, escopo, limites e a organização responsável pelo processo de GR.

Estas etapas estão divididas nos seguintes grupos:

- **Critérios básicos**: Seleção ou desenvolvimento de um método para GR levando em conta critérios de avaliação de riscos, critérios de

impacto e critérios de aceitação de riscos. Além disto, a organização deve avaliar se existem recursos disponíveis para:

- Executar a análise/avaliação de riscos e estabelecer um plano de tratamento dos mesmos;
- Definir e implementar políticas e procedimentos, incluindo implementação dos controles selecionados;
- Monitorar controles;
- Monitorar o processo de GR de SI.

- **Critérios para a avaliação de riscos**: Segundo a norma NBR ISO 27005, os critérios para avaliação de riscos devem ser definidos com base em cinco itens, sendo dois deles relacionados abaixo:
  - O valor estratégico do processo que trata as informações de negócio;
  - A criticidade dos ativos de informação envolvidos.
- **Critérios de impacto**: Desenvolvimento dos critérios para avaliação dos impactos, levando em consideração o montante de danos ou custos à organização proveniente de algum evento relacionado com a Segurança da Informação (SI).
- **Critérios para a aceitação do risco**: Desenvolvimento dos critérios para aceitação dos riscos, sendo que frequentemente eles devem depender das políticas, metas e objetivos da organização bem como os interesses das partes interessadas. Para estabelecimento dos critérios de aceitação do risco, os itens abaixo devem ser levados em consideração:
  - Critérios de negócio;
  - Aspectos legais e regulatórios;
  - Operações;
  - Tecnologia;
  - Financeiras;
  - Fatores sociais e humanitários.
- **Escopo e limites:** A organização deve definir o escopo do processo de GR de SI, sendo que deve garantir que todos os ativos relevantes sejam analisados e avaliados além da definição dos limites do processo. Qualquer exclusão do escopo deve ser justificada.

- **Organização para gestão de riscos de segurança da informação:** A organização e as responsabilidades para o processo de GR de SI devem ser estabelecidas. Esta organização deve ser aprovada pelos gestores apropriados, sendo que abaixo segue dois exemplos dos papéis e responsabilidades dessa organização:
    - Identificação e análise das partes interessadas;
    - Definição de alçadas para a tomada de decisões.

4.1.2 Análise/avaliação de risco de segurança da informação

A organização deve selecionar o seu próprio método para análise e avaliação de riscos baseado nos objetivos e na meta de análise e avaliação de riscos. As principais ações dessa etapa se dividem em Análise de riscos (Identificação de riscos e Estimativa de riscos) e Avaliação de riscos, sendo elas descritas nos itens a seguir.

4.1.2.1 Análise de riscos

A atividade de Análise de riscos é dividida em duas partes sendo elas a Identificação de riscos e Estimativa de riscos.

4.1.2.1.1 Identificação de riscos

Nesta atividade é necessário determinar eventos que possam causar perda potencial e deixar claro como, onde e por que a perda pode acontecer.

4.1.2.1.2 Identificação dos ativos

Para a identificação dos ativos deve-se detalhar a identificação de ativos com várias informações, sendo cada um deles identificados com o seu responsável, localidade e todas as informações pertinentes para a sua mais adequada identificação. Todos os ativos dentro do escopo devem ser identificados.

- **Entradas:** Escopo e limites para a análise/avaliação de riscos. Lista de componentes com todas as informações de sobre o responsável.
- **Saídas:** Lista de ativos com riscos a serem gerenciados e lista de processos de negócios relacionados aos ativos e suas relevâncias.

4.1.2.1.3 Identificação de ameaças

É recomendado que a organização busque listas de ameaças genéricas em catálogos externos, este processo pode auxiliar na identificação de ameaças comuns. Todas as avaliações anteriores de ameaças devem ser levadas em consideração.

- **Entradas:** Informações sobre ameaças a partir da análise crítica de incidentes de segurança da informação, dos responsáveis pelos ativos, incluindo fontes externas de ameaças.
- **Saídas:** Uma listagem com todas as ameaças identificadas separadas por tipo e fonte.

4.1.2.1.4 Identificação dos controles existentes

Em todas as organizações alguns controles de gestão de riscos já são utilizados, algumas vezes estão desatualizados ou não estão mais em funcionamento. Nesta atividade todos os controles existentes devem ser identificados para evitar retrabalho e garantir que estes controles existentes estão funcionando corretamente. Os controles ineficazes, insuficientes ou não justificáveis devem ser identificados e avaliados para uma possível remoção.

- **Entradas:** Documentação referente aos controles existentes na organização e os planos de implementação do tratamento do risco.
- **Saídas:** Listagem de todos os controles existentes e planejados com as informações de sua implementação e status de utilização.

4.1.2.1.5 Identificação das vulnerabilidades

As vulnerabilidades de todos os ativos devem ser identificadas, sendo que uma vulnerabilidade que não tenha uma ameaça relacionada a ela pode não causar prejuízo, mas deve ser identificada e monitorada. Vulnerabilidades decorrentes de diferentes fontes devem ser consideradas, por exemplo, as intrínsecas ao ativo e as extrínsecas.

- **Entradas:** Listagem de ameaças conhecidas, listagem de ativos identificados e listagem de controles existentes.
- **Saídas:** Listagem de vulnerabilidades relacionadas com os ativos, listagem de vulnerabilidades relacionadas às ameaças e controles existentes, listagem de vulnerabilidades que não tenham nenhuma ameaça relacionada.

4.1.2.1.6 Identificação das consequências

A organização deve identificar as consequências operacionais de cenários de incidentes relacionados a segurança da informação, sendo que esta identificação deve contemplar as consequências de perda de confidencialidade, integridade e disponibilidade. As consequências devem ser identificadas, por exemplo, em função de oportunidades perdidas, tempo de trabalho perdido, dentre outras.

- **Entradas:** Listagem de ativos, listagem de processos de negócio e listagem de ameaças e vulnerabilidades.
- **Saídas:** Listagem de cenários de incidentes com suas consequências associadas aos ativos e processos de negócio.

4.1.2.1.7 Estimativa de riscos

Para a estimativa de riscos, a organização deve definir qual metodologia para a estimativa de riscos será utilizada sendo que duas metodologias podem ser

utilizadas, a qualitativa e a quantitativa. É possível utilizar ambas as metodologias em conjunto.

- **Metodologia qualitativa:** A metodologia qualitativa utiliza escala de atributos qualificadores para consequências potencias como, por exemplo, pequena, média e grande em conjunto com a probabilidade dessas consequências ocorrerem. A sua vantagem é o fácil entendimento por qualquer pessoa, mas a sua desvantagem é a dependência à escolha subjetiva da escala.
- **Metodologia quantitativa:** Com a metodologia quantitativa é utilizado uma escala com valores numéricos tanto para as consequências quanto para as probabilidades. Na maioria dos casos a estimativa quantitativa utiliza dados históricos de incidentes sendo que sua vantagem é estar relacionada diretamente aos objetivos e interesses da organização. Uma das desvantagens da estimativa quantitativa é a falta de dados sobre novos riscos ou sobre fragilidades da segurança da informação.

4.1.2.1.8 Avaliação das consequências

Todos os ativos da organização devem ter a sua valorização determinada em função do impacto ao negócio, sendo esta valorização de preferência efetuada de forma quantitativa. Deve ser avaliado o impacto sobre o negócio da organização causado por um incidente de segurança da informação, levando em consideração as consequências como, por exemplo, a perda de confidencialidade.

- **Entradas:** Listagem de cenários de incidentes identificados como relevantes contendo:
  - Identificação das ameaças;
  - Vulnerabilidades;
  - Ativos afetados;
  - Consequências para os ativos e processos de negócio.

- **Saídas:** Listagem de consequências avaliadas referentes a um cenário de incidente, relacionadas aos ativos e critérios de impacto.

4.1.2.1.9 Avaliação da probabilidade dos incidentes

Nesta atividade é necessário avaliar a probabilidade de cada cenário de incidentes identificado e do impacto relacionado usando as metodologias de estimativa qualitativa e quantitativas. Para a avaliação da probabilidade de incidentes deve-se levar em conta a frequência da ocorrência das ameaças e a facilidade com que as vulnerabilidades podem ser exploradas.

- **Entradas:** Listagem de todos os cenários identificados como relevantes contendo a identificação das ameaças, vulnerabilidades exploradas, ativos afetados e consequências para os ativos e processos do negócio. Listagem com todos os controles planejados e executados contendo a eficácia, implementação e status de sua utilização.
- **Saídas:** Probabilidade de todos os cenários identificados.

4.1.2.1.10 Estimativa do nível do risco

A estimativa do nível do risco deve ser baseada nas consequências e na probabilidade estimada nas atividades anteriores. Segundo a norma NBR ISO 27005, o risco estimado é uma combinação entre a probabilidade de um cenário de incidente e suas consequências.

- **Entradas:** Listagem de cenários de incidentes com suas consequências relacionadas aos ativos, processos de negócio e suas probabilidades.
- **Saídas:** Listagem de riscos com a sua estimativa definida.

4.1.2.2 Avaliação de riscos

Como atividade final da etapa de Análise/Avaliação de risco de segurança da informação, a avaliação de riscos deve comparar os riscos estimados com os critérios de avaliação e critérios de aceitação do risco definidos na etapa de Definição de Contexto. Esta atividade tem como foco principal efetuar a avaliação do risco baseada principalmente no nível de riscos aceitável, ou seja, a organização definirá linhas de base para que ao ultrapassar determinado valor, o risco será aceito ou imediatamente definido que deverá ser tratado.

- **Entradas:** Listagem de riscos contendo a sua estimativa e critérios para a avaliação de riscos.
- **Saídas:** Listagem de riscos ordenados por prioridade e associados aos cenários de incidentes que os provocam.

4.1.3 Tratamento do risco de segurança da informação

A etapa de tratamento do risco de segurança da informação é efetuada após todos os passos de identificação, análise e avaliação de riscos, sendo estes riscos tratados para minimizar as possíveis perdas da organização. Esta etapa contém quatro opções para o tratamento do risco: a Redução do risco, Retenção do risco, Ação de evitar o risco e Transferência do risco.

Segundo a norma NBR ISO 27005, a figura 8 demonstra a atividade de tratamento do risco dentro do processo de gestão de riscos de segurança da informação.

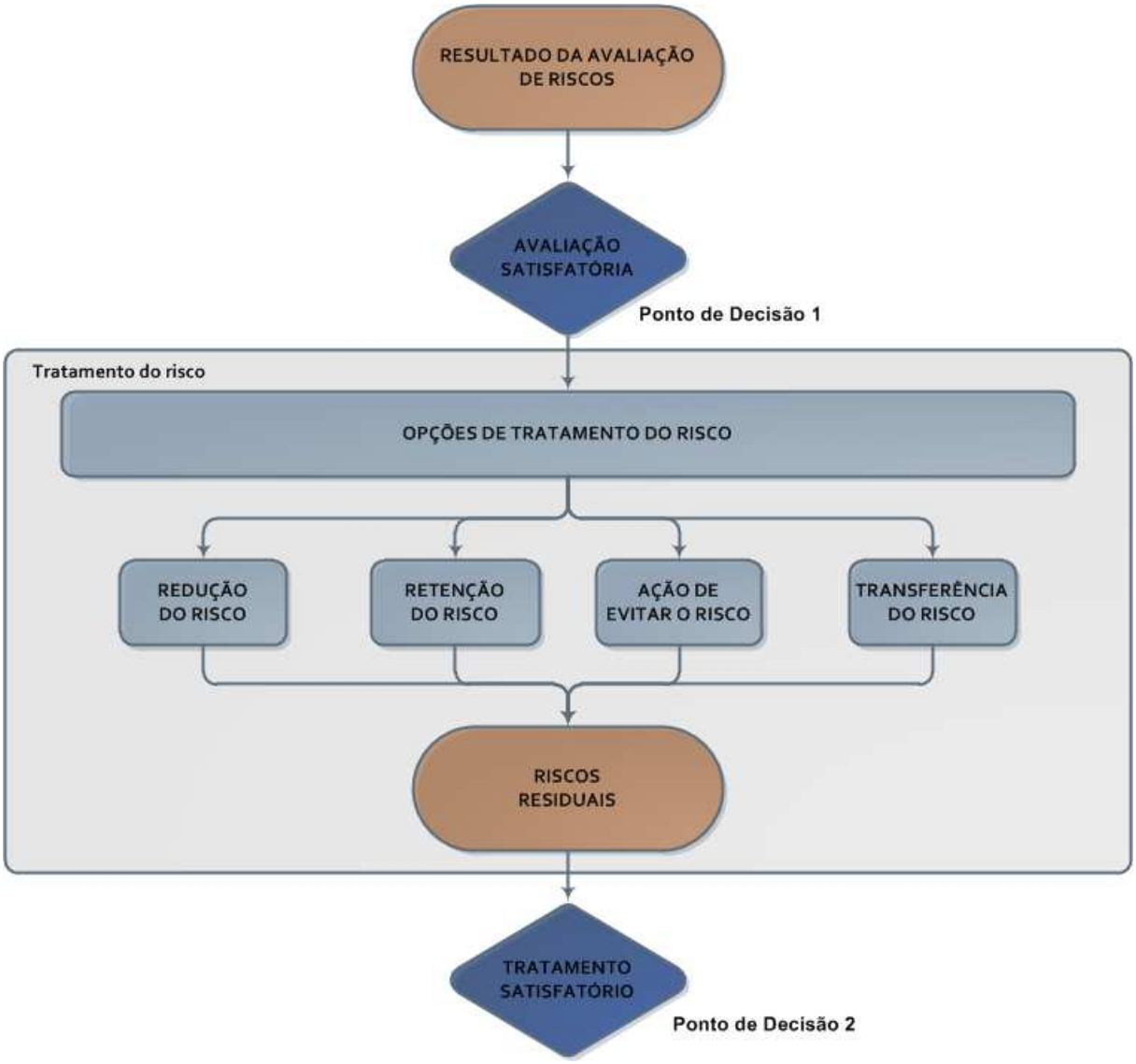

Figura 8 - A atividade de tratamento de riscos segundo a norma NBR ISO 27005.
Fonte: NBR ISO 27005 (ABNT, 2008).

As principais saídas desta atividade são o plano de tratamento do risco e os riscos residuais, sendo que ambos devem ser aceitos e aprovados pelos gestores da organização.

4.1.3.1 Redução do risco

Nesta atividade é efetuada a redução do risco através da seleção de controles até que o risco residual possa ser reavaliado e considerado aceitável. É necessário avaliar o custo benefício de um controle implementado em relação ao valor dos ativos que estão sendo protegidos. Para a implementação de controles, várias restrições devem ser consideradas, sendo abaixo listadas algumas delas:

- Restrições técnicas
- Restrições culturais
- Restrições ambientais
- Facilidade de uso
- Restrições de recursos humanos

4.1.3.2 Retenção do risco

A organização aceita as perdas relacionadas ao risco conforme critérios para aceitação do risco, não sendo necessário implementar controles para este risco, onde todas as decisões devem ser tomadas com base na avaliação de riscos satisfazendo as políticas e objetivos da organização.

4.1.3.3 Ação de evitar o risco

Quando alguma opção de tratamento do risco exceder os benefícios, pode-se optar por evitar o risco, ou seja, a organização pode optar pela eliminação de uma atividade planejada ou existente para evitar que o risco ocorra. Segundo a norma NBR ISO 27005, um exemplo seriam os riscos causados por fenômenos naturais, onde o custo-benefício poderia ser maior movendo fisicamente as instalações de processamento de dados para um local onde não existe o risco ou este está sob controle.

4.1.3.4 Transferência do risco

O risco pode ser transferido para outra entidade que possa gerenciá-lo de forma mais eficaz. A transferência de riscos pode criar novos riscos ou modificar os existentes, sendo necessário um novo tratamento do risco. As responsabilidades legais pelas consequências do risco continuarão sendo da organização. Segundo a norma NBR ISO 27005, um exemplo de transferência de risco seria a contratação de um seguro protegendo a organização das consequências.

4.1.4 Aceitação do risco de segurança da informação

Os planos de tratamento do risco e os riscos residuais devem ser aprovados, onde esta aprovação deve ser registrada formalmente em conjunto com a decisão de aceitar os riscos. Caso identificado que os critérios para aceitação do risco sejam inadequados ou incompletos, os gestores podem aceitar o risco desde que esta decisão seja registrada e justificada do motivo pelo qual não foi possível utilizar os critérios normais para aceitação do risco. A saída principal desta atividade é uma listagem dos riscos aceitos, contendo uma justificativa para aqueles riscos que foram aceitos sem utilizar os critérios normais para a aceitação do risco.

4.1.5 Comunicação do risco de segurança da informação

A organização deve garantir que a percepção do risco das partes interessadas, bem como a sua percepção dos benefícios sejam identificadas e documentadas e que as razões subjacentes sejam claramente entendidas e consideradas.

As informações sobre os riscos devem ser trocadas e compartilhadas entre o tomador de decisões e as partes interessadas, sendo necessária a criação de planos de comunicação para operações rotineiras como também para situações mais graves. A coordenação desta comunicação entre os tomadores de decisões e as partes interessadas, é feita através de uma comissão criada pela organização, onde os riscos, a sua priorização, formas adequadas de tratá-los e sua aceitação podem ser discutidos amplamente.

A atividade de comunicação do risco deve ser um processo contínuo dentro da organização.

4.1.6 Monitoramento e análise crítica de riscos de segurança da informação

Dentro do *PDCA* do SGSI de uma organização, a atividade de Monitoramento e análise crítica de riscos de segurança da informação está relacionada com a fase de “Agir”, conforme já mencionado no presente trabalho.

Nesta atividade a organização irá executar ações corretivas e preventivas obtidas das análises críticas das partes interessadas e dos gestores pertinentes. Este monitoramento e análise estão divididos em duas sessões, sendo elas descritas abaixo.

4.1.6.1 Monitoramento e análise crítica dos fatores de risco

Todos os riscos e seus fatores, ou seja, valores de ativos, impactos, ameaças, vulnerabilidades e probabilidade de ocorrências devem ser monitorados e analisados criticamente continuamente para verificar possíveis alterações. É necessário, dentro da atividade, revisar constantemente riscos antes avaliados como baixos ou aceitáveis para verificar se não houve mudanças na avaliação. Se necessári,o é possível utilizar serviços de terceiros para avaliar mudanças em ameaças ou vulnerabilidade, agilizando o processo. O objetivo principal desta atividade é um alinhamento contínuo da gestão de riscos com os objetivos de negócio da organização e com os critérios para a aceitação do risco.

4.1.6.2 Monitoramento e análise crítica e melhoria do processo de gestão de riscos

A organização deve monitorar todos os processos de GR de SI para propor as mudanças e melhorias necessárias nos processos, focando em mantê-los atualizados e consistentes em relação ao contexto, resultado da análise/avaliação de riscos, tratamento do risco bem como os planos de gestão. Qualquer melhoria ou ações necessárias para melhorar a conformidade do processo, devem ser comunicadas aos gestores apropriados para as validações pertinentes ao processo. Esta atividade visa em garantir a relevância permanente dos processos de GR de SI para os objetivos de negócios da organização ou atualização do processo.

4.2 Gestão de Riscos de Segurança da Informação com o processo “Avaliar e Gerenciar os Riscos de TI” (PO9) do CobiT 4.1

Igualmente a norma NBR ISO 27005, o CobiT 4.1 também implementa uma gestão de riscos para as organizações, sendo que os requisitos do processo P09 “Avaliar e Gerenciar os Riscos de TI” e suas métricas serão descritas a seguir neste capítulo.

Para todos os processos do CobiT, duas perguntas são de extrema importante para definição clara do objetivo que este processo tem para a organização, no caso do processo P09 “Avaliar e Gerenciar os Riscos de TI”, as perguntas com suas respectivas respostas seguem abaixo:

- Quais os requisitos do negócio este processo deve atender?
  - Efetuar a análise e comunicação dos riscos de TI e seus possíveis impactos para os processos e objetivos de negócio.
- Qual será o foco deste processo?
  - Desenvolvimento de uma estrutura de gerenciamento de riscos integrada ao gerenciamento de riscos corporativo e operacional com a intenção de avaliar, mitigar e comunicar riscos residuais.

Para o atingimento do objetivo de GR de SI, o CobiT divide o seu processo P09 em objetivos de controles, conforme itens abaixo:

4.2.1 P09.1 Alinhamento da gestão de riscos de TI e de Negócios

Neste objetivo de controle do CobiT, é necessário que a GR de SI esteja alinhada a gestão de riscos da organização. O processo de gestão de riscos de forma genérica, para qualquer tipo de riscos, é tratado na norma ISO/IEC 31000:2009 conforme já citado no presente trabalho, é uma norma de gestão de riscos genéricos o que pode ser utilizada para o gerenciamento de riscos da organização de forma geral.

4.2.2 P09.2 Estabelecimento do Contexto de Risco

A organização deve estabelecer o contexto ao qual a estrutura de gerenciamento de risco será aplicada, buscando atingir os objetivos esperados. Esta definição de contexto deve levar em consideração o cenário interno e externo de cada avaliação de risco, objetivo da avaliação e os critérios utilizados para a avaliação dos riscos em questão. O estabelecimento de contexto serve para a organização deixar claro qual será o foco do trabalho, qual o escopo do gerenciamento e os critérios básicos de avaliação dos riscos.

4.2.3 P09.3 Identificação de Eventos

Todos os eventos com um potencial de impacto negativo para as operações e para os objetivos da organização devem ser identificados, devendo incluir aspectos de:

- Negócios;
- Regulamentações;
- Jurídicos;
- Tecnologia;
- Parcerias de negócios;
- Recursos humanos;
- Operacionais.

Nesta etapa é importante que todos os riscos que podem explorar alguma vulnerabilidade relevante, devem ser identificados. As informações da natureza do impacto devem ser registradas e estes registros mantidos, bem como manter um registro do histórico dos riscos relevantes já identificados.

4.2.4 P09.4 Avaliação do Risco

Conforme o P09.3, nesta etapa de Avaliação do Risco os riscos já foram identificados, sendo necessário agora uma avaliação regular da probabilidade e do impacto de todos os riscos identificados utilizando os métodos qualitativo e

quantitativo. Os riscos antes classificados como residuais e inerentes, devem receber uma avaliação de probabilidade e impactos individualmente, por categoria e com base no portfólio da organização.

4.2.5 P09.5 Resposta ao Risco

Depois de efetuado os processos de identificação e avaliação dos riscos, a organização deve desenvolver estratégias para garantir que controles com o adequado custo-benefício, mitiguem os riscos de forma contínua, sendo que estas estratégias devem evitar, reduzir, compartilhar ou aceitar o risco. O objetivo de controle de resposta ao risco deve também determinar responsabilidades e levar em consideração todos os critérios de tolerância definidos nos processos anteriores.

4.2.6 P09.6 Manutenção e Monitoramento do Plano de Ação de Risco

Neste objetivo de controle as atividade de controle de todos os níveis da organização devem ser priorizadas e planejadas para implementar o objetivo de controle de resposta ao risco, focando nos riscos identificados como necessários de tratamento, levando em consideração os custos, benefícios e responsabilidades pela execução.

As ações assumidas pelos donos dos processos afetados devem ser executadas, sendo este processo responsável pelo controle da execução destas ações, qualquer alteração na execução dos planos a Alta Direção deve ser informada. As aprovações das ações recomendadas bem como a aceitação dos riscos residuais devem ser obtidas.

4.2.7 Modelo de maturidade – P09 Avaliar e Gerenciar os Riscos de TI

No capítulo 2 do presente trabalho, foi apresentado o modelo de maturidade genérico utilizado pelo CobiT 4.1 para avaliação da maturidade. Para avaliar a maturidade de GR de SI nas organizações, o CobiT 4.1 utiliza um modelo específico para riscos, sendo ele informado abaixo:

- **Nível 0 – Inexistente:** Não acontece avaliação de risco para processos e decisões de negócio. A organização não considera os impactos no negócio associados a vulnerabilidades da segurança e incertezas de projetos de desenvolvimento. Gerenciar riscos não é considerado relevante para adquirir soluções ou entregar serviços de TI.
- **Nível 1 – Inicial / *Ad hoc*:** Os riscos de TI são considerados de forma *ad hoc*. Avaliações informais de risco de projeto são realizadas quando solicitadas em cada projeto. Avaliações de risco são às vezes identificadas em um plano de projeto, mas raramente atribuídas aos gerentes correspondentes. Riscos específicos relacionados a TI, como segurança, disponibilidade e integridade, são ocasionalmente considerados nos projetos. Os riscos de TI que afetam o dia-a-dia da operação são raramente discutidos em reuniões gerenciais. Mesmo onde os riscos são levantados, as ações para mitigá-los são inconsistentes. Está surgindo um entendimento de que os riscos de TI são importantes e devem ser considerados.
- **Nível 2 – Repetível, porém Intuitivo:** Existe uma abordagem imatura e inicial de avaliação de risco utilizada a critério de alguns gerentes de projeto. A gestão de risco é superficial e geralmente aplicada somente a grandes projetos ou em resposta a problemas. O processo de mitigação de risco está começando a ser implementado onde são identificados riscos.
- **Nível 3 – Processo definido:** Uma política corporativa de gestão de risco define onde e como conduzir as avaliações de risco. A gestão de risco segue um processo definido e documentado. Há treinamento em gestão de risco disponível para todo o pessoal. Decisões de seguir o processo de gestão de risco e receber treinamento são deixadas a critério de cada indivíduo. A metodologia de avaliação de risco é convincente, robusta e assegura a identificação dos riscos–chave para o negócio. Um processo para mitigar os riscos-chave é implementado após a identificação dos riscos. As responsabilidades pela gestão de riscos estão definidas nas descrições de cargo.

- **Nível 4 – Gerenciável e Mensurável:** A avaliação e a gestão de risco são procedimentos padronizados. As exceções do processo de gestão de risco são relatadas à Diretoria de TI. A gestão de risco de TI é uma responsabilidade da Alta Direção. O risco é avaliado e mitigado no nível de projeto e também regularmente no nível de operação de TI. O comitê executivo é avisado das mudanças no ambiente de negócios e de TI que podem afetar consideravelmente os cenários de riscos relacionados a TI. A Diretoria é capaz de monitorar a posição do risco e tomar decisões fundamentadas no nível de exposição aceitável. Todos os riscos identificados têm um responsável definido, e o comitê executivo e a Diretoria de TI estabeleceram os níveis de risco que a organização irá tolerar. A área de TI desenvolveu indicadores padrão para avaliar riscos e definir taxas de riscos/retornos. A área de TI aloca recursos para um projeto de gestão de risco operacional a fim de reavaliar periodicamente os riscos. Um banco de dados de gestão de risco é estabelecido, e uma parte dos processos de gerenciamento de risco está começando a ser automatizada. A área de TI estuda estratégias de mitigação de riscos.
- **Nível 5 – Otimizado:** O gerenciamento de risco atingiu um estágio de desenvolvimento em que há um processo organizacional estruturado em vigor e bem gerenciado. Boas práticas são aplicadas em toda a organização. A captura, a análise e o relato de dados de gestão de risco estão altamente automatizados. É recebida orientação de lideranças da área, e a organização de TI participa de grupos de discussão para troca de experiências. A gestão de risco está totalmente integrada às operações de negócio e de TI, é bem aceita e envolve extensivamente os usuários dos serviços de TI. A Direção de TI detecta e age quando grandes decisões operacionais e de investimentos de TI são tomadas sem considerar o plano de gestão de risco. A Direção de TI avalia continuamente as estratégias de mitigação de risco.

4.2.8 Métricas de monitoramento

Para garantir que o processo de GR de SI funcione de forma adequada, o CobiT 4.1 propõe uma série de métricas (indicadores) para medir o desempenho do processo. Estas métricas estão divididas em três grupos de objetivos, sendo eles Objetivos de TI, Objetivos de Processos e Objetivos das Atividades onde cada objetivo é descrito abaixo em conjunto com as suas respectivas métricas:

- **Objetivos de TI:**
  - Percentual de objetivos críticos de TI cobertos por avaliações de risco;
  - Percentual de avaliações críticas de TI integradas a abordagem de gestão de riscos de TI.
- **Objetivos de Processos:**
  - Percentual de riscos críticos de TI identificados que tenham sido avaliados criticamente;
  - Quantidade de novos riscos críticos de TI identificados (comparado com o exercício anterior);
  - Quantidade de incidentes significativos causados por riscos não identificados no processo de gestão de riscos;
  - Percentual de riscos críticos de TI identificados que tenham planos de ação desenvolvidos.
- **Objetivos das Atividades:**
  - Percentual do orçamento de TI gasto nas atividades de gestão de riscos (avaliação crítica e mitigação);
  - Frequência de revisão dos processos de gestão de riscos de TI;
  - Percentual de avaliações de riscos críticas aprovadas;
  - Quantidade de relatórios de monitoração de riscos em um determinado período;
  - Percentual de eventos de TI identificados que são utilizados nas avaliações de risco críticas;
  - Percentual dos planos de ação de gestão de risco aprovados para implementação.

4.2.9 Entradas e Saídas

Os processos do CobiT 4.1 recebem informações de outros processos da mesma forma que enviam informações para os demais. As entradas e saídas do P09 “Avaliar e Gerenciar os Riscos de TI” são informadas abaixo conforme figura 9:

Origem	Entrada
PO1	Planejamentos estratégico e tático de TI; Portfólio de serviços de TI;
PO10	Plano de gerenciamento de risco de projetos;
DS2	Riscos de fornecedores;
DS4	Resultados dos testes de contingência;
DS5	Vulnerabilidades e ameaças de segurança;
ME1	Histórico de eventos e tendências de riscos;
ME4	Grau aceitável corporativo de riscos de TI

Saída	Destino						
Avaliação crítica de riscos;	PO1	DS4	DS5	DS12	ME4		
Relatório de riscos;	ME4						
Diretrizes para a gestão de riscos de TI;	PO6						
Planos de ação para remediação de riscos de TI	PO4	AI6					

Figura 9 - Entradas e Saídas do P09 - Avaliar e Gerenciar os Riscos de TI.
Fonte: CobiT (2007).

5 ALINHAMENTO ENTRE NBR ISO 27005:2008 E COBIT 4.1

Neste capítulo serão apresentadas duas tabelas de alinhamento, sendo a tabela 3 o alinhamento da norma NBR ISO 27005 com o CobiT 4.1 e a tabela 4 o alinhamento entre o CobiT 4.1 com a norma NBR ISO 27005.

O foco destes alinhamentos são todos os requisitos da norma NBR ISO 27005 e o processo P09 “Avaliar e Gerenciar os Riscos de TI”, sendo que estão contempladas as entradas e saídas deste processo.

Em ambas as tabelas de alinhamento, as lacunas entre a norma NBR ISO 27005 e o CobiT foram sinalizadas de vermelho tachado, indicando que o requisito avaliado não é atendido por uma das partes.

5.1 Alinhamento da norma NBR ISO/IEC 27005:2008 com CobiT 4.1

Na tabela 3 é indicado o alinhamento entre a norma NBR ISO/IEC 27005:2008 com o CobiT 4.1 com o foco em Gestão de Riscos de Segurança da Informação.

Esta tabela relaciona todos os requisitos da norma NBR ISO 27005 e qual a sua relação com o processo P09 “Avaliar e Gerenciar os Riscos de TI”, incluindo as entradas e saídas do mesmo.

Na coluna “Pontos principais” são descritos os tópicos mais importantes do requisito avaliado, sendo que se faz necessário consultar a norma NBR ISO 27005 para total compreensão dos itens inclusos no requisito.

Tabela 3 - Alinhamento norma NBR ISO/IEC 27005:2008 com CobiT 4.1

ABNT NBR ISO/IEC 27005:2008			CobiT 4.1	
Item	**Tópico da norma NBR ISO/IEC 27005**	**Pontos principais**	**Objetivo de controle**	**Processos de TI**
7	**Definição de contexto**			
7.1	Considerações gerais	Estabelecer o contexto da GR de SI; Determinar o propósito da GR para a SI.	PO9.2 Estabelecimento do Contexto de Risco	PO9 Avaliar e Gerenciar os Riscos de TI
7.2	Critérios básicos	Selecionar ou desenvolver um método para GR levando em conta critérios de avaliação de riscos, critérios de impacto e critérios de aceitação de riscos.	PO9.2 Estabelecimento do Contexto de Risco	PO9 Avaliar e Gerenciar os Riscos de TI
7.2	Critérios para avaliação de riscos	Definir os critérios para avaliação de riscos.	PO9.2 Estabelecimento do Contexto de Risco	PO9 Avaliar e Gerenciar os Riscos de TI
7.2	Critérios de impacto	Desenvolver os critérios para avaliação dos impactos, levando em consideração o montante de danos ou custos à organização proveniente de algum evento relacionado a SI.	PO9.4 Avaliação de Risco	PO9 Avaliar e Gerenciar os Riscos de TI
7.2	Critérios para aceitação do risco	Desenvolver os critérios para aceitação dos riscos, frequentemente eles devem depender das políticas, metas e objetivos da organização bem como os interesses das partes interessadas.	ME4.5 Gestão de Riscos	ME4 Prover Governança de TI
7.3	Escopo e limites	Definir o escopo do processo de GR de SI; Garantir que todos os ativos relevantes sejam analisados e avaliados; Determinar os limites; Justificar todas as exclusões do escopo.	PO9.2 Estabelecimento do Contexto de Risco	PO9 Avaliar e Gerenciar os Riscos de TI
7.4	Organização para gestão de riscos de SI	Definir e estabelecer as responsabilidade do processo de GR de SI; Aprovar organização com gestores apropriados.	PO4.8 Responsabilidade por Riscos, Segurança e Conformidade	PO4 Definir os Processos, Organização e Relacionamentos de TI
8	**Análise/avaliação de risco de segurança da informação**			
8.1	Descrição geral do processo de análise/avaliação de riscos de segurança da informação	A organização deve selecionar seu próprio método para análise/avaliação de riscos baseados nos objetivos e na meta da análise/avaliação de riscos.	PO9.4 Avaliação de Risco	PO9 Avaliar e Gerenciar os Riscos de TI

Tabela 3 - Alinhamento norma NBR ISO/IEC 27005:2008 com CobiT 4.1 (Continuação)

ABNT NBR ISO/IEC 27005:2008			CobiT 4.1	
Item	**Tópico da norma NBR ISO/IEC 27005**	**Pontos principais**	**Objetivo de controle**	**Processos de TI**
8.2	***Análise de riscos***			
8.2.1	***Identificação de riscos***			
8.2.1.1	Introdução à identificação de riscos	Determinar eventos que possam causar perda potencial e deixar claro como, onde e por que a perda pode acontecer.	PO9.3 Identificação de Eventos	PO9 Avaliar e Gerenciar os Riscos de TI
8.2.1.2	Identificação dos ativos	Identificar todos os ativos dentro do escopo definido; Identificar um responsável para cada ativo.		
8.2.1.3	Identificação das ameaças	Identificar as ameaças e suas fontes; Utilizar ameaças genéricas buscadas em listas ou catálogos externos.	PO9.3 Identificação de Eventos	PO9 Avaliar e Gerenciar os Riscos de TI
8.2.1.4	Identificação dos controles existentes	Identificar controles existentes e garantir que estão em funcionamento; Identificar controles ineficazes, insuficientes ou não justificados e avaliar a remoção.		
8.2.1.5	Identificação das vulnerabilidades	Identificar todas as vulnerabilidades que podem ser exploradas por ameaças.	PO9.3 Identificação de Eventos	PO9 Avaliar e Gerenciar os Riscos de TI
8.2.1.6	Identificação das consequências	Identificar as consequências de perda de confidencialidade, integridade e disponibilidade.	PO9.3 Identificação de Eventos	PO9 Avaliar e Gerenciar os Riscos de TI
8.2.2	***Estimativa de riscos***			
8.2.2.1	Metodologia para a estimativa de riscos	Definir a metodologia para estimativa de riscos, podendo ser utilizada uma das duas: Qualitativa ou Quantitativa (ou ambas)	PO9.4 Avaliação de Risco	PO9 Avaliar e Gerenciar os Riscos de TI
8.2.2.2	Avaliação das consequências	Avaliar o impacto sobre o negócio da organização causado por um incidente, levando em consideração as consequências, como por exemplo, a perda da confidencialidade. Determinar a valorização dos ativos em função do impacto ao negócio, de preferência de forma quantitativa.	PO9.4 Avaliação de Risco	PO9 Avaliar e Gerenciar os Riscos de TI

Tabela 3 - Alinhamento norma NBR ISO/IEC 27005:2008 com CobiT 4.1 (Continuação)

ABNT NBR ISO/IEC 27005:2008			CobiT 4.1	
Item	**Tópico da norma NBR ISO/IEC 27005**	**Pontos principais**	**Objetivo de controle**	**Processos de TI**
8.2.2.3	Avaliação da probabilidade dos incidentes	Avaliar a probabilidade de cada cenário de incidente e do seu impacto correspondente.	PO9.4 Avaliação de Risco	PO9 Avaliar e Gerenciar os Riscos de TI
8.2.2.4	Estimativa do nível de risco	Estimar o nível de risco para todos os cenários considerados relevantes. Estimativa deve ser baseada nas consequências e na probabilidade estimada.		
8.3	***Avaliação de riscos***	Comparar os riscos estimados com os critérios de avaliação de riscos.	PO9.4 Avaliação de Risco	PO9 Avaliar e Gerenciar os Riscos de TI
9	**Tratamento do risco de segurança da informação**			
9.1	Descrição geral do processo de tratamento do risco	Determinar os riscos residuais após o tratamento do risco e elaborar um Plano de Tratamento do risco.	PO9.5 Resposta ao Risco	PO9 Avaliar e Gerenciar os Riscos de TI
			PO9.6 Manutenção e Monitoramento do Plano de Ação de Risco	PO9 Avaliar e Gerenciar os Riscos de TI
9.2	Redução do risco	Redução do risco através da seleção de controles até que o risco residual possa ser reavaliado e considerado aceitável. O custo benefício de um controle implementado em relação ao valor dos ativos que estão sendo protegidos deve ser avaliado.	PO9.5 Resposta ao Risco	PO9 Avaliar e Gerenciar os Riscos de TI
9.3	Retenção do risco	Tomar decisões sobre retenção de riscos com base na avaliação de riscos. Se o nível do risco atender aos critérios de aceitação do risco não há necessidade de implementar controles adicionar e pode haver a retenção do risco.	PO9.5 Resposta ao Risco	PO9 Avaliar e Gerenciar os Riscos de TI
9.4	Ação de evitar o risco	Caso alguma opção de tratamento do risco exceder os benefícios, pode-se optar por evitar o risco.	PO9.5 Resposta ao Risco	PO9 Avaliar e Gerenciar os Riscos de TI
9.5	Transferência do risco	Transferir o risco para outra entidade que possa gerenciá-lo de forma mais eficaz, dependendo da avaliação de riscos.	PO9.5 Resposta ao Risco	PO9 Avaliar e Gerenciar os Riscos de TI

Tabela 3 - Alinhamento norma NBR ISO/IEC 27005:2008 com CobiT 4.1 (Continuação)

ABNT NBR ISO/IEC 27005:2008			CobiT 4.1	
Item	**Tópico da norma NBR ISO/IEC 27005**	**Pontos principais**	**Objetivo de controle**	**Processos de TI**
10	**Aceitação do risco de segurança da informação**	Efetuar a decisão de aceitar os riscos e registrar formalmente. Aprovar planos propostos de tratamento de riscos e riscos residuais resultantes e registrar essa aprovação.	PO9.6 Manutenção e Monitoramento do Plano de Ação de Risco	PO9 Avaliar e Gerenciar os Riscos de TI
11	**Comunicação do risco de segurança da informação**	Trocar e compartilhar as informações sobre os riscos com as partes interessadas e tomadores de decisão. Realizar a atividade de comunicação do risco continuamente.	PO6.2 Risco de TI Corporativo e Estrutura Interna de Controle	PO6 Comunicar Metas e Diretrizes Gerenciais
12	**Monitoramento e análise crítica de riscos de segurança da informação**			
12.1	Monitoramento e análise crítica dos fatores de risco	Monitorar e analisar criticamente os riscos e seus fatores; Revisar constantemente riscos antes avaliados como baixo ou aceitáveis para verificar se não houve mudanças na avaliação.		
12.2	Monitoramento, análise crítica e melhoria do processo de gestão de riscos	Monitorar, analisar e melhorar continuamente o processo de GR de SI. Monitoramento do contexto para verificações de mudanças e alterações em riscos.	ME1 Monitorar e Avaliar o Desempenho de TI (Todos os Objetivos de controle)	ME1 Monitorar e Avaliar o Desempenho de TI
			PO9.6 Manutenção e Monitoramento do Plano de Ação de Risco	PO9 Avaliar e Gerenciar os Riscos de TI

5.2 Alinhamento do CobiT 4.1 com a norma NBR ISO/IEC 27005:2008

Conforme citado no inicio deste capitulo, a tabela 4 é o alinhamento entre o CobiT 4.1 e a norma NBR ISO 27005 com foco na GR de SI.

Para o alinhamento completo, as entradas e saídas do processo P09 “Avaliar e Gerenciar os Riscos de TI” foram incluídas e alinhadas com a norma.

Com a tabela 4 é possível identificar as lacunas presentes entre o CobiT 4.1 e a norma NBR ISO 27005, auxiliando no entendimento dos requisitos necessários entre os dois.

A coluna de “Pontos principais” indica os tópicos mais relevantes dentro do Objetivo de Controle avaliado, sendo que estes tópicos devem ser consultados diretamente no documento do CobiT 4.1 para o seu total entendimento, o objetivo da tabela 4 é visualização das lacunas presentes entre o CobiT 4.1 e a norma NBR ISO 27005 para a GR de SI, não a total interpretação do requisito que está sendo avaliado.

Tabela 4 - Alinhamento do CobiT 4.1 com a norma NBR ISO/IEC 27005:2008

CobiT 4.1			ABNT NBR ISO/IEC 27005:2008	
Objetivo de controle	**Processos de TI**	**Pontos principais**	**Item**	**Tópico da norma NBR ISO/IEC 27005**
PO9.1 Alinhamento da gestão de riscos de TI e de Negócios	PO9 Avaliar e Gerenciar os Riscos de TI	Gestão de riscos deve ser alinhada aos objetivos da organização, bem como uma gestão de riscos mais abrangente, dos riscos que não sejam somente de TI.	5	Contextualização
PO9.2 Estabelecimento do Contexto de Risco	PO9 Avaliar e Gerenciar os Riscos de TI	Estabelecer o contexto da GR de SI na organização. Definir contexto interno e externo. Definir os critérios para avaliação de riscos.	7.1	Considerações gerais
			7.2	Critérios básicos
			7.2	Critérios para avaliação de riscos
			7.3	Escopo e limites
PO9.3 Identificação de Eventos	PO9 Avaliar e Gerenciar os Riscos de TI	Identificar todas as ameaças ativas que estão explorando alguma vulnerabilidade com potencial impacto para a organização. Determinar a natureza dos impactos. Registrar e manter um histórico dos riscos considerados relevantes.	8.2.1.1	Introdução à identificação de riscos
			8.2.1.3	Identificação das ameaças
			8.2.1.5	Identificação das vulnerabilidades
PO9.4 Avaliação de Risco	PO9 Avaliar e Gerenciar os Riscos de TI	Avaliar a probabilidade e impacto dos riscos identificados dentro dos contextos definidos. Efetuar a avaliação utilizando métodos qualitativos e quantitativos. Riscos aceitos (inerentes e residuais) devem ser avaliados individualmente, organizados por categorias.	7.2	Critérios de impacto
			8.1	Descrição geral do processo de análise/avaliação de riscos de segurança da informação
			8.2.2.1	Metodologia para a estimativa de riscos
			8.2.2.2	Avaliação das consequências
			8.2.2.3	Avaliação da probabilidade dos incidentes
			8.3	Avaliação de riscos

Tabela 4 - Alinhamento do CobiT 4.1 com a norma NBR ISO/IEC 27005:2008 (Continuação)

CobiT 4.1			ABNT NBR ISO/IEC 27005:2008	
Objetivo de controle	**Processos de TI**	**Pontos principais**	**Item**	**Tópico da norma NBR ISO/IEC 27005**
PO9.5 Resposta ao Risco	PO9 Avaliar e Gerenciar os Riscos de TI	Definir e desenvolver um processo de resposta ao risco, identificando estratégias de riscos, como evitar, reduzir, compartilhar ou aceitar o risco. Determinar responsabilidades e considerar os níveis de tolerância anteriormente definidos.	9	Tratamento do risco de segurança da informação
PO9.6 Manutenção e Monitoramento do Plano de Ação de Risco	PO9 Avaliar e Gerenciar os Riscos de TI	Priorizar e planejar atividades de controle para implementações de resposta aos riscos. Identificar os custos, benefícios e responsabilidades pela execução da resposta ao risco. Obter aprovação para execução das ações recomendadas. Obter o aceite do responsável pelo processo de negócio ameaçado pelo risco que foi aceito e pelas ações definidas e aprovadas. Monitorar a execução dos planos de ações definidos para a manutenção dos riscos identificados e reporte caso necessário para Alta Direção.	9.1	Descrição geral do processo de tratamento do risco
			10	Aceitação do risco de segurança da informação
			12.2	Monitoramento, análise crítica e melhoria do processo de gestão de riscos
ENTRADAS do PO9 Avaliar e Gerenciar os Riscos de TI				
PO1.4 Plano Estratégico de TI	PO1 Definir um Plano Estratégico de TI	Criar um plano estratégico que defina como a TI contribuirá com os objetivos estratégicos da organização e quais os custos e riscos relacionados. Este plano estratégico deve ser detalhado para possibilitar a definição e criação dos planos táticos de TI.		

Tabela 4 - Alinhamento do CobiT 4.1 com a norma NBR ISO/IEC 27005:2008 (Continuação)

CobiT 4.1			ABNT NBR ISO/IEC 27005:2008	
Objetivo de controle	**Processos de TI**	**Pontos principais**	**Item**	**Tópico da norma NBR ISO/IEC 27005**
PO1.5 Planos Táticos de TI	PO1 Definir um Plano Estratégico de TI	Criação de um portfólio de planos táticos de TI proveniente do plano estratégico de TI, sendo que estes planos táticos devem descrever quais as ações e recursos serão necessários e como uso dos recursos e os benefícios serão monitorados e administrados.		
PO1.6 Gerenciamento do Portfólio de TI	PO1 Definir um Plano Estratégico de TI	Gerenciar o portfólio de programas de investimentos de TI em conjunto com as áreas de negócio da organização. Identificar, definir, avaliar, priorizar, selecionar, iniciar, gerenciar e controlar os programas.		
PO10.9 Gestão de Risco do Projeto	PO10 Gerenciar Projetos	Eliminar ou minimizar riscos que podem ocorrer a cada projeto, sendo que os riscos devem ser identificados pelo processo de Gestão de Projetos e os resultados esperados do projeto devem ser estabelecidos e registrados centralmente.		
DS2.3 Gerenciamento de Riscos do Fornecedor	DS2 Gerenciar Serviços Terceirizados	Identificar e minimizar os riscos relativos à capacidade de fornecimento contínuo dos fornecedores de forma segura e eficiente. Contratos devem estar em conformidade com padrões universais, acordos de confidencialidade, garantias, condições gerais, conformidade com requisitos de segurança, dentre outros, devem ser considerados no gerenciamento de riscos do fornecedor.		

Tabela 4 - Alinhamento do CobiT 4.1 com a norma NBR ISO/IEC 27005:2008 (Continuação)

CobiT 4.1			ABNT NBR ISO/IEC 27005:2008	
Objetivo de controle	**Processos de TI**	**Pontos principais**	**Item**	**Tópico da norma NBR ISO/IEC 27005**
DS4.5 Teste do Plano de Continuidade de TI	DS4 Assegurar a Continuidade dos Serviços	Efetuar testes com o plano de continuidade de TI com frequência para garantir que os sistemas de TI possam ser recuperados da forma esperada. Os resultados dos testes devem ser registrados e os planos de ação para alguma eventual alteração no plano de continuidade deve ser implementado.		
DS5.2 Plano de Segurança de TI	DS5 Garantir a Segurança dos Sistemas	Efetuar a tradução dos requisitos de negócio, de risco e conformidade em um único plano abrangente de segurança de TI.		
ME1.4 Avaliação de Desempenho	ME1 Monitorar e Avaliar o Desempenho de TI	Avaliar e analisar periodicamente o desempenho com base nas metas, efetuar análises de causa-raiz de problemas e caso necessário iniciar ações corretivas para tratar causas desconhecidas.	12.1	Monitoramento e análise crítica dos fatores de risco
ME4.5 Gestão de Riscos	ME4 Prover Governança de TI	Definir em conjunto com o conselho diretor qual o apetite corporativo por riscos de TI além de obter uma segurança referente as práticas de GR de SI são suficientes para que os riscos atuais de TI não ultrapassem o apetite definido pela Alta Direção.	10	Aceitação do risco de segurança da informação
			12.2	Monitoramento, análise crítica e melhoria do processo de gestão de riscos
SAÍDAS do PO9 Avaliar e Gerenciar os Riscos de TI				
PO1.4 Plano Estratégico de TI	PO1 Definir um Plano Estratégico de TI	Criar um plano estratégico que defina como a TI contribuirá com os objetivos estratégicos da organização e quais os custos e riscos relacionados. Este plano estratégico deve ser detalhado para possibilitar a definição e criação dos planos táticos de TI.		

Tabela 4 - Alinhamento do CobiT 4.1 com a norma NBR ISO/IEC 27005:2008 (Continuação)

CobiT 4.1			ABNT NBR ISO/IEC 27005:2008	
Objetivo de controle	**Processos de TI**	**Pontos principais**	**Item**	**Tópico da norma NBR ISO/IEC 27005**
DS4.2 Planos de Continuidade de TI	DS4 Assegurar a Continuidade dos Serviços	Desenvolver planos de continuidade de TI com o objetivo de reduzir os possíveis impactos de uma grande interrupção dos processos de negócio da organização. Estes de planos devem ser baseados no risco de possíveis impactos no negócio, sendo que devem contemplar os requisitos de capacidade de restabelecimento, processamento alternativo e capacidade de recuperação de todas as operações críticas da TI.		
DS5.2 Plano de Segurança de TI	DS5 Garantir a Segurança dos Sistemas	Efetuar a tradução dos requisitos de negócio, de risco e conformidade em um único plano abrangente de segurança de TI.		
DS12.1 Seleção do Local e Layout	DS12 Gerenciar o Ambiente Físico	Definir e selecionar um local apropriado para os equipamentos de TI, levando em consideração os riscos associados a desastres naturais e não naturais além de avaliar as leis e regulamentações relevantes.	8.2.1.3	Identificação das ameaças
			8.3	Avaliação de riscos
			9	Tratamento do risco de segurança da informação
DS12.2 Medidas de Segurança Física	DS12 Gerenciar o Ambiente Físico	Definir e implementar medidas de segurança físicas com o objetivo de proteger os ativos críticos de TI dos riscos relacionados a roubo, temperatura, fogo, dentre outros.	8.2.1.3	Identificação das ameaças
			8.3	Avaliação de riscos
			9	Tratamento do risco de segurança da informação
ME4.5 Gestão de Riscos	ME4 Prover Governança de TI	Definir em conjunto com o conselho diretor qual o apetite corporativo por riscos de TI além de obter uma segurança referente as práticas de GR de SI são suficientes para que os riscos atuais de TI não ultrapassem o apetite definido pela Alta Direção.	10	Aceitação do risco de segurança da informação
			12.2	Monitoramento, análise crítica e melhoria do processo de gestão de riscos

Tabela 4 - Alinhamento do CobiT 4.1 com a norma NBR ISO/IEC 27005:2008 (Continuação)

CobiT 4.1			ABNT NBR ISO/IEC 27005:2008	
Objetivo de controle	**Processos de TI**	**Pontos principais**	**Item**	**Tópico da norma NBR ISO/IEC 27005**
ME4.6 Medição de Desempenho	ME4 Prover Governança de TI	Monitorar se os objetivos de TI foram atingidos ou excedidos ou se o progresso na direção dos mesmos atende as expectativas. A Alta Direção deve ser reportada com os portfólios, programas e desempenho de TI através de relatórios gerenciais.		
PO6.2 Risco de TI Corporativo e Estrutura Interna de Controle	PO6 Comunicar Metas e Diretrizes Gerenciais	Desenvolver e manter uma estrutura para estabelecer uma abordagem completa dos riscos e controles da TI alinhada com as políticas e com o ambiente de controle de TI, bem como a estrutura de riscos e controles da organização.	11	Comunicação do risco de segurança da informação
PO4.8 Responsabilidade por Riscos, Segurança e Conformidade	PO4 Definir os Processos, Organização e Relacionamentos de TI	A organização deve definir e atribuir todos os papéis críticos para o gerenciamento dos riscos de TI, por exemplo, responsabilidade sobre segurança física, conformidade, etc. Obter orientação junto a Diretoria sobre os níveis de riscos de TI aceitáveis e a aprovação de todos os riscos residuais.	7.4	Organização para gestão de riscos de SI
AI6.2 Avaliação de Impacto, Priorização e Autorização	AI6 Gerenciar Mudanças	Todas as mudanças devem ser avaliadas quanto o possível risco que possa causar. Todas as mudanças devem ser categorizadas, priorizadas e autorizadas.		

6 MODELO ESTRUTURADO PARA GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

Um dos grandes desafios de uma área de TI é a implementação de uma GR de SI alinhada a mais de um *framework* ou norma, efetuando em algumas ocasiões ações dispersas, sem controle efetivo ou preocupação com algumas etapas básicas para a sua efetiva implementação.

As tabelas 3 e 4 indicam o alinhamento entre o *framework* CobiT 4.1 em conjunto com a norma NBR ISO 27005, sendo que neste alinhamento é possível identificar que nenhum dos dois é totalmente completo, o que sugere a utilização de ambos em conjunto.

Com a necessidade de implementar uma GR de SI alinhada ao *framework* CobiT 4.1 e a norma NBR ISO 27005, a tabela 5 demonstra um Modelo estruturado para Gestão de Riscos de Segurança da Informação, dividido em 11 etapas, sendo elas descritas abaixo:

- **ETAPA 1 -** Definição do Planejamento e Gerenciamento de TI
- **ETAPA 2 -** Definição de Responsabilidades
- **ETAPA 3 -** Definição do escopo e contexto
- **ETAPA 4 -** Definição de Critérios de Impacto, Avaliação e Aceitação de Riscos
- **ETAPA 5 -** Identificação de Riscos e Eventos
- **ETAPA 6 -** Estimativa de Riscos
- **ETAPA 7 -** Avaliação de Riscos
- **ETAPA 8 -** Tratamento e Resposta ao Risco
- **ETAPA 9 -** Aceitação de Riscos e Riscos residuais
- **ETAPA 10 -** Controle e Comunicação do Processo de Gestão de Riscos
- **ETAPA 11 -** Monitoramento e Melhoria contínua do Processo de Gestão de Riscos

Este modelo tem como objetivo orientar os gestores responsáveis pela implementação de um processo de GR de SI nas organizações, sendo que no modelo é descrito os requisitos e as principais ações, dentro de cada etapa.

Todas as etapas do modelo incluem a lista dos requisitos da norma NBR ISO 27005 ou Objetivos de Controle do CobiT 4.1 aos quais ela está relacionada, onde as lacunas estão sinalizadas em vermelho tachado, indicando que o requisito não é contemplado.

As etapas estão divididas e ordenadas em função da necessidade de implementação em uma sequência definida, como, por exemplo, a etapa de Avaliação de Riscos não pode ser executada antes da etapa de Identificação de Riscos e Eventos.

O modelo não tem como objetivo eliminar a interpretação, análise e avaliação da norma NBR ISO 27005 bem como do CobiT 4.1 em sua totalidade, mas servir de apoio na implementação da GR de SI alinhada com ambos.

Além das etapas e ações indicadas na tabela 5, é necessária a implementação das métricas de controle e monitoramento do CobiT 4.1, conforme indicado no item 4.2.8 Métricas de monitoramento do presente trabalho.

Tabela 5 - Modelo estruturado para Gestão de Riscos de Segurança da Informação

Descrição dos requisitos / Principais ações	ABNT NBR ISO/IEC 27005:2008		CobiT 4.1	
	Item	Tópico da norma NBR ISO/IEC 27005	Objetivo de controle	Processos de TI
ETAPA 1 - Definição do Planejamento de TI				
• Desenvolver Planos de Continuidade de TI baseados no risco de possíveis impactos no negócio. • Efetuar a tradução dos requisitos de negócio, de risco e conformidade em um único plano abrangente de segurança de TI. • Criar um Plano Estratégico de TI que defina como a TI contribuirá com os objetivos estratégicos da organização e quais os custos e riscos relacionados. • Criação de Planos Táticos de TI provenientes do Plano Estratégico de TI sendo que estes planos devem descrever as ações, a alocação e administração de recursos. • Efetuar o gerenciamento do portfólio de programas de investimento de TI. • Alinhar a Gestão de Riscos de TI com a gestão de riscos da organização como um todo, não focando somente em TI.			DS4.2 Planos de Continuidade de TI	DS4 Assegurar a Continuidade dos Serviços
			DS5.2 Plano de Segurança de TI	DS5 Garantir a Segurança dos Sistemas
			PO1.4 Plano Estratégico de TI	PO1 Definir um Plano Estratégico de TI
			PO1.5 Planos Táticos de TI	PO1 Definir um Plano Estratégico de TI
			PO1.6 Gerenciamento do Portfólio de TI	PO1 Definir um Plano Estratégico de TI
			PO9.1 Alinhamento da gestão de riscos de TI e de Negócios	PO9 Avaliar e Gerenciar os Riscos de TI
ETAPA 2 - Definição de Responsabilidades				
• Definir, estabelecer e atribuir todas as responsabilidades e papéis críticos para o processo de Gestão de Risco. • Aprovar com gestores apropriados a organização definida e registrar formalmente.	7.4	Organização para gestão de riscos de SI	PO4.8 Responsabilidade por Riscos, Segurança e Conformidade	PO4 Definir os Processos, Organização e Relacionamentos de TI
ETAPA 3 - Definição do escopo e contexto				
• Definir o contexto da GR de SI. • Determinar os limites, garantir que todos os ativos	7.1	Considerações gerais	PO9.2 Estabelecimento do	PO9 Avaliar e Gerenciar os Riscos de TI

Descrição dos requisitos / Principais ações	ABNT NBR ISO/IEC 27005:2008		CobiT 4.1	
	Item	Tópico da norma NBR ISO/IEC 27005	Objetivo de controle	Processos de TI
relevantes sejam analisados e avaliados. • Justificar as possíveis exclusões do escopo. • Definir o contexto interno e externo da GR de SI.	7.3	Escopo e limites	Contexto de Risco	
ETAPA 4 - Definição de Critérios de Impacto, Avaliação e Aceitação de Riscos				
• Definir os critérios para avaliação de riscos. • Definir os critérios para avaliação de impactos considerando o possível dano ou custos à organização proveniente de algum evento relacionado a SI. • Definir os critérios para aceitação do risco.	7.2	Critérios básicos	PO9.2 Estabelecimento do Contexto de Risco	PO9 Avaliar e Gerenciar os Riscos de TI
	7.2	Critérios para avaliação de riscos		
	7.2	Critérios de impacto	PO9.4 Avaliação de Risco	PO9 Avaliar e Gerenciar os Riscos de TI
	7.2	Critérios para aceitação do risco	PO4.8 Responsabilidade por Riscos, Segurança e Conformidade	PO4 Definir os Processos, Organização e Relacionamentos de TI
ETAPA 5 - Identificação de Riscos e Eventos				
• Determinar quais os eventos podem causar perdas potenciais, deixando claro como, onde e por que a perda pode ocorrer. • Identificar todos os ativos dentro do escopo/contexto definidos. • Identificar as ameaças e as suas fontes relacionadas. • Identificar controles existentes, avaliar a sua eficácia e funcionamento, caso necessário, efetuar uma avaliação para a possível remoção do controle. • Identificar todas as vulnerabilidade relacionadas as ameaças. • Identificar as consequências de perda de confidencialidade, integridade e disponibilidade. • Armazenar histórico dos riscos considerados relevantes. • Identificar os riscos que podem ocorrer a cada	8.2.1	Identificação de riscos	PO9.3 Identificação de Eventos	PO9 Avaliar e Gerenciar os Riscos de TI
	8.2.1.1	Introdução à identificação de riscos	PO10.9 Gestão de Risco do Projeto	PO10 Gerenciar Projetos
	8.2.1.2	Identificação dos ativos	DS2.3 Gerenciamento de Riscos do Fornecedor	DS2 Gerenciar Serviços Terceirizados
	8.2.1.3	Identificação das ameaças	DS12.1 Seleção do Local e Layout	DS12 Gerenciar o Ambiente Físico

Descrição dos requisitos / Principais ações	ABNT NBR ISO/IEC 27005:2008		CobiT 4.1	
	Item	Tópico da norma NBR ISO/IEC 27005	Objetivo de controle	Processos de TI
Projeto, sendo estes necessários de tratamento para a sua mitigação. • Identificar e minimizar os riscos relativos à capacidade de fornecimento contínuo dos fornecedores da organização de forma segura e eficiente. • Identificar os possíveis riscos do local onde os equipamentos de TI serão alocados, levando em consideração riscos associados a desastres naturais e não naturais. • Identificar os riscos de segurança física para a proteção dos ativos críticos de TI no ambiente físico.	8.2.1.4	Identificação dos controles existentes		
	8.2.1.5	Identificação das vulnerabilidades	DS12.2 Medidas de Segurança Física	DS12 Gerenciar o Ambiente Físico
	8.2.1.6	Identificação das consequências		
ETAPA 6 - Estimativa de Riscos				
• Definir a metodologia para estimativa de riscos, podendo ser utilizada a metodologia qualitativa ou quantitativa, além de ser possível utilizar as duas juntas. • Estimar o nível de risco para cada cenário considerado, sendo que a estimativa deve ser baseada nas consequências e na probabilidade estimada.	8.2.2.1	Metodologia para a estimativa de riscos		
	8.2.2.4	Estimativa do nível de risco		
ETAPA 7 - Avaliação de Riscos				
• Definir qual será a metodologia utilizada para avaliação de riscos. • Avaliar o impacto nos negócios da organização causado por um incidente de segurança da informação, sendo que é necessário levar em consideração as consequências, como por exemplo,	8.1	Descrição geral do processo de análise/avaliação de riscos de segurança da informação	PO9.4 Avaliação de Risco	PO9 Avaliar e Gerenciar os Riscos de TI

Descrição dos requisitos / Principais ações	ABNT NBR ISO/IEC 27005:2008		CobiT 4.1	
	Item	Tópico da norma NBR ISO/IEC 27005	Objetivo de controle	Processos de TI
a perda de confidencialidade. • Determinar a valorização dos ativos dentro do contexto e escopo definidos em função do impacto ao negócio. • Avaliar a probabilidade da ocorrência de incidentes. • Efetuar uma comparação entre os riscos estimados com os critérios de avaliação de riscos. • Efetuar a avaliação de riscos inerentes e residuais de forma individual e organizados por categoria. • Qualquer mudança deve ser avaliada quanto aos possíveis riscos que possa causar, sendo que devem ser categorizadas, priorizadas e autorizadas pelos gestores pertinentes. • Avaliar os possíveis riscos do local onde os equipamentos de TI serão alocados, levando em consideração riscos associados a desastres naturais e não naturais. • Avaliar os riscos de segurança física para a proteção dos ativos críticos de TI no ambiente físico.	8.2.2.2	Avaliação das consequências	AI6.2 Avaliação de Impacto, Priorização e Autorização	AI6 Gerenciar Mudanças
	8.2.2.3	Avaliação da probabilidade dos incidentes	DS12.1 Seleção do Local e Layout	DS12 Gerenciar o Ambiente Físico
	8.3	Avaliação de riscos	DS12.2 Medidas de Segurança Física	DS12 Gerenciar o Ambiente Físico
ETAPA 8 - Tratamento e Resposta ao Risco				
• Determinar quais são os riscos residuais. • Elaborar e definir um Plano de Tratamento e Resposta ao Risco. • Efetuar a redução de riscos até que seja reavaliado e considerável aceitável. • Efetuar a retenção do risco quando possível com base nos critérios de avaliação de riscos. • Quando pertinente ou alguma opção de tratamento do risco exceder os benefícios, o mesmo pode ser evitado. • Transferir o risco para outra entidade que possa gerenciá-lo de forma mais eficaz, levando em consideração os critérios de avaliação de riscos.	9.1	Descrição geral do processo de tratamento do risco	PO9.5 Resposta ao Risco	PO9 Avaliar e Gerenciar os Riscos de TI
	9.2	Redução do risco		
	9.3	Retenção do risco		
	9.4	Ação de evitar o risco		
	9.5	Transferência do risco		

Descrição dos requisitos / Principais ações	ABNT NBR ISO/IEC 27005:2008		CobiT 4.1	
	Item	Tópico da norma NBR ISO/IEC 27005	Objetivo de controle	Processos de TI
ETAPA 9 - Aceitação de Riscos e Riscos residuais				
• Determinar, analisar e avaliar todos os riscos residuais. • Efetuar a decisão de aceitar os riscos residuais e registrar formalmente a aprovação junto aos gestores pertinentes. • Obter a aprovação do responsável pelo processo de negócio ameaçado pelo risco que foi aceito e pelas ações definidas. • Aprovar planos de tratamento de riscos, registrando as decisões tomadas. • Definir junto ao Conselho Diretor da organização qual o apetite corporativo por riscos e obter aprovação referente às práticas de GR de SI, garantindo que os riscos residuais não ultrapassem o limite definido pela Alta Direção.	9.1	Descrição geral do processo de tratamento do risco	PO9.6 Manutenção e Monitoramento do Plano de Ação de Risco	PO9 Avaliar e Gerenciar os Riscos de TI
	10	Aceitação do risco de segurança da informação	ME4.5 Gestão de Riscos	ME4 Prover Governança de TI
ETAPA 10 - Controle e Comunicação do Processo de Gestão de Riscos				
• Desenvolver uma estrutura para efetuar a troca e compartilhamento de informações sobre a GR de SI com as partes interessadas e os tomadores de decisão. • Efetuar o processo de comunicação para as partes interessadas de forma contínua.	11	Comunicação do risco de segurança da informação	PO6.2 Risco de TI Corporativo e Estrutura Interna de Controle	PO6 Comunicar Metas e Diretrizes Gerenciais
ETAPA 11 - Monitoramento e Melhoria contínua do Processo de Gestão de Riscos				
• Monitorar e analisar criticamente os riscos e seus fatores. • Revisar continuamente os riscos avaliados como baixo ou aceitáveis para verificar possíveis mudanças na avaliação. • Monitorar o contexto e o escopo para verificar	12	Monitoramento e análise crítica de riscos de segurança da informação	PO9.6 Manutenção e Monitoramento do Plano de Ação de Risco	PO9 Avaliar e Gerenciar os Riscos de TI

Descrição dos requisitos / Principais ações	ABNT NBR ISO/IEC 27005:2008		CobiT 4.1	
	Item	Tópico da norma NBR ISO/IEC 27005	Objetivo de controle	Processos de TI
possíveis mudanças e alterações em riscos. • Monitorar se os objetivos de TI foram atingidos ou excedidos e efetuar o reporte para a Alta Direção através de relatórios gerenciais. • Monitorar a execução das ações definidas para tratamento e manutenção dos riscos identificados. • Periodicamente avaliar e analisar o desempenho do processo de GR de SI com base em metas definidas, efetuar análises de causa-raiz de problemas e caso necessário abrir planos de ação para tratar as causas. • Efetuar testes com o Plano de Continuidade de TI para garantir que os sistemas de TI possam ser recuperados da forma esperada. Todos os resultados devem ser registrados e planos de ação abertos para tratar qualquer possível necessidade de alteração no Plano de Continuidade de TI. • Monitorar, analisar e melhorar continuamente o processo de GR de SI.	12.1	Monitoramento e análise crítica dos fatores de risco	ME4.6 Medição de Desempenho	ME4 Prover Governança de TI
	12.2	Monitoramento, análise crítica e melhoria do processo de gestão de riscos	ME1.4 Avaliação de Desempenho	ME1 Monitorar e Avaliar o Desempenho de TI
			DS4.5 Teste do Plano de Continuidade de TI	DS4 Assegurar a Continuidade dos Serviços

7 CONSIDERAÇÕES FINAIS

Atualmente é evidente a dependência das organizações das suas informações e seus ativos, sendo que os riscos que os cercam crescem a cada dia. Devido a isto várias organizações iniciam um processo de implementação de GR de SI, algumas vezes forçadas por alguma lei, regulamentação, norma ou por identificação interna de necessidade de melhoria na gestão.

O presente trabalho teve como objetivo principal elaborar um modelo estruturado em etapas para auxiliar na implementação de GR de SI alinhada ao CobiT 4.1 e a norma NBR ISO 27005, sendo ele apresentado no capítulo 6. Com este trabalho foi possível concluir que um *framework* ou norma não é suficientemente completo no que tange a GR de SI na sua totalidade, ficando alguma etapa não efetuada ou até mesmo com pouca exigência para sua execução, deixando clara assim a necessidade de alinhar mais de um *framework* ou norma para a criação de uma GR de SI efetiva.

O Modelo Estruturado para Gestão de Riscos de Segurança da Informação pode auxiliar gestores na implementação da GR de SI, separado em 11 etapas, sendo todas elas alinhadas a norma NBR ISO 27005 e ao CobiT 4.1, com os principais pontos e ações a serem executadas, agilizando assim o processo de implementação e focando as ações de forma estruturada e organizada.

Para ampliar o Modelo Estruturado para Gestão de Riscos de Segurança da Informação, a continuação do presente trabalho no futuro será a inclusão dos requisitos exigidos pelo *framework Information Technology Infrastructure Library* (ITIL), atualmente na versão 3, ampliando assim a visão do modelo, buscando a total aderência a norma NBR ISO 27005, CobiT 4.1 e ITIL v3.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **Gestão de Riscos – Vocabulário – Recomendação para uso em normas**: NBR ISO/IEC Guia 73:2005. Rio de Janeiro: ABNT, 2005.

_____. **Código de Prática para a Gestão da Segurança da Informação**: NBR ISO/IEC 27002:2005. Rio de Janeiro: ABNT, 2005a.

_____. **Sistemas de Gestão de Segurança da Informação - Requisitos:** NBR ISO/IEC 27001:2006. Rio de Janeiro: ABNT, 2006.

_____.**Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação:** NBR ISO/IEC 27005:2008. São Paulo: ABNT, 2008.

_____.**Gestão de riscos - Princípios e diretrizes:** NBR ISO/IEC 31000:2009. Rio de Janeiro: ABNT, 2009.

ANDRADE, Maria Margarida de. **Como Preparar Trabalhos para Cursos de Pós-Graduação**. 5 ed. São Paulo: Altas, 2002.

HEISER, Jay. **Quatro erros comuns na gestão de riscos**. 2009. Disponível em: <http://www.b2bmagazine.com.br/b2bmagazine/Portugues/detNoticia.php?codnoticia=24414> Acesso em 10 de abr. de 2010

B2B Magazine. **Segurança da Informação começa no papel.** 2009. Disponível em: <http://www.b2bmagazine.com.br/b2bmagazine/Portugues/detNoticia.php?codnoticia=24374> Acesso em 10 de abr. de 2010

BARROS, Aidil Jesus Paes de; LEHFELD, Neide Aparecida de Souza. Projeto **de Pesquisa: Propostas Metodológicas**. 13 ed. Editora Vozes. 1990.

GIL, Antônio C. **Métodos e técnicas de pesquisa social.** São Paulo: Atlas, 1999.

INFOSEC COUNCIL. **Planejamento Estratégico da Segurança da Informação**. São Paulo: Infosec Council, 2010. Disponível em: <http://www.infoseccouncil.org.br/publicacoes/201001_whitePaper_PlanejamentoPT.pdf> Acesso em 10 de abr. de 2010

IT GOVERNANCE INSTITUTE (ITGI). **CobiT® 4.1**. Estados Unidos: ITGI, 2007. Disponível em: < http://www.isaca.org/Content/NavigationMenu/Members_and_Leaders1/COBIT6/Obtain_COBIT/cobit41_portuguese.pdf >. Acesso em: 24 mar. 2010.

_____. **Aligning CobiT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit**. Estados Unidos: ITGI, 2007. Disponível em: http://www.isaca.org/Knowledge-Center/Research/Documents/Aligning-COBIT,ITILV3,ISO27002-Bus-Benefit-12Nov08-Research.pdf> Acesso em 24 de mai. de 2010.

KROLL, Josiane. **Um Modelo conceitual para Especificação da Gestão de Riscos de Segurança em Sistemas de Informação.** Santa Maria: Dissertação de mestrado apresentada à Universidade Federal de Santa Maria, 2010.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. **Fundamentos de metodologia científica.** 4.ed. rev. e ampl. São Paulo: Atlas, 2001.

LEOPARDI, Maria Tereza. **Metodologia da pesquisa na saúde.** Santa Maria: Pallotti, 2001.

MARTINS, Gilberto de Andrade. **Estudo de Caso. Uma Estratégia de Pesquisa.** São Paulo: Atlas, 2006.

MARTINS, Gilberto de Andrade. **Manual para Elaboração de Monografias e Dissertações**. 3 ed., São Paulo: Atlas, 2002.

MAYER, Janice. **Um Modelo para avaliar o Nível de Maturidade do processo de Gestão De Riscos em Segurança da Informação.** São Leopoldo: Monografia apresentada à Universidade do Vale do Rio dos Sinos, 2008.

MÓDULO SECURITY. **10ª Pesquisa Nacional de Segurança da Informação**. São Paulo: Módulo Security, 2007. Disponível em: <http://www.modulo.com.br/media/10a_pesquisa_nacional.pdf > Acesso em 10 de abr. de 2010.

NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR. **Pesquisa Sobre o uso das Tecnologias da Informação e da Comunicação no Brasil 2008.** São Paulo: 2009. Disponível em: <http://www.cetic.br/tic/2008/index.htm> Acesso em 10 de abr. de 2010.

OLIVEIRA, Silvio Luiz. **Tratado de Metodologia Científica**. 2 ed. São Paulo Pioneira, 1998.

ROESCH, Maria Azevedo. **Projetos de Estágio e de Pesquisa em Administração:** guia para estágios, trabalhos de conclusão, dissertações e estudos de caso. São Paulo: 1996.

SALES, João Rufino de. **Formação de Cultura em Segurança da Informação**. São Paulo: Infosec Council, 2010. Disponível em: <http://www.infoseccouncil.org.br/publicacoes/200608_whitePaper_Formacao.pdf> Acesso em 10 de abr. de 2010.

SÊMOLA, Marcos. **Gestão da Segurança da Informação**: uma visão executiva da segurança da informação: aplicada ao security officer. Rio de Janeiro: Campus, 2003.

VERGARA, Sylvia Constant. **Projetos e relatórios de pesquisa em Administração.** São Paulo: Atlas, 2004.

YIN, Robert K. **Estudo de caso:** planejamento e métodos. 3.ed. Porto Alegre: Bookman, 2005.