Proposta de um Modelo para Avaliar o Nível de Maturidade do Processo de Gestão de Riscos em Segurança da Informação

Janice Mayer, Leonardo Lemes Fagundes

Universidade do Vale do Rio dos Sinos (UNISINOS)
Av. Unisinos, 950 – CEP 93.022-000 – São Leopoldo – RS – Brasil
j.mayer@brturbo.com.br, llemes@unisinos.br

Abstract. *Risk Management (RM) are coordinated activities to direct and control an organization with regard to risk, and that includes analysis, evaluation, treatment, acceptance and risks reporting. The organization needs to implement RM in a reliable and methodical way in compliance to regulations, norms and laws, and also need to fulfill mandatory requisites in the information security field. However, there is no maturity model that measures and assesses the maturity level of this process. The objective of the present work is to suggest and to specify a model for assessment of Enterprises' maturity level regarding the RM process and Information Security.*

Resumo. *Gestão de Riscos (GR) são atividades coordenadas para direcionar e controlar uma organização no que se refere a riscos, isso inclui a análise, a avaliação, o tratamento, a aceitação e a comunicação de riscos. As organizações precisam implementar GR de forma consistente e sistemática, para buscar conformidades com as leis, normas e regulamentações, bem como atender a requisitos obrigatórios da área de segurança da informação. No entanto, não há um modelo de maturidade que meça ou avalie o nível de maturidade desse processo. O objetivo desse artigo é propor e especificar um modelo para avaliar o nível de maturidade das empresas em relação ao processo de GR em Segurança da Informação.*

1. Introdução

Ao longo das últimas décadas a informação se tornou um dos ativos mais valiosos para as organizações, a ponto de que o vazamento ou a indisponibilidade da informação colocar em risco a execução de processos de negócios vitais. Esse cenário se torna ainda mais crítico com o crescente aumento das vulnerabilidades associadas aos diversos ativos (que oferecem suporte aos processos de negócios das empresas) e com o surgimento, em grande escala, de ameaças capazes de explorar essas vulnerabilidades [Sêmola 2003]. Para enfrentar essa realidade é exigido das organizações o desenvolvimento de recursos e processos cada vez mais eficientes para manter as informações seguras [Módulo S*ecurity* 2007]. Neste contexto a gestão de riscos representa um recurso essencial para que a empresa possa estimar ameaças, vulnerabilidades e impactos.

O *risco* é a probabilidade de ameaças explorarem vulnerabilidades, gerando perdas de confidencialidade, integridade e disponibilidade, causando possivelmente

impactos (conseqüências) nos negócios. Já o processo de *gestão de riscos* compreende um conjunto de atividades coordenadas para direcionar e controlar uma organização no que se refere a riscos [ABNT 2005a].

Segundo Santos (2008), a gestão de riscos é implementada para aumentar a eficiência operacional, reduzindo assim, perdas como fraudes, falhas, sinistros e acidentes, conduzindo a empresa a uma melhoria nos seus processos. Com base em uma análise mais detalhada e focada na área de Tecnologia da Informação (TI) pode-se observar que atualmente a maior parte das instituições entende que a análise de riscos é uma forma de atender aos requisitos impostos pelas leis, normas e regulamentações relacionadas com a segurança da informação [Módulo S*ecurity* 2007], como (1) o Acordo da Basiléia II [R*isk Bank* 2002], (2) a Lei *Sarbanes-Oxley* [Santos e Lemes 2004] e (3) a resolução 3380/BACEN [BCB 2006].

No contexto específico da área de segurança da informação, a gestão de riscos trata-se, por exemplo, de um requisito obrigatório para (4) a implementação de um SGSI (Sistema de Gestão de Segurança da Informação) [ABNT 2005], (5) serve como insumo para a elaboração da análise do impacto nos negócios – etapa preliminar à criação das estratégias de contingência [BSI 2006] e também (6) como um importante recurso para as organizações que buscam conformidade com padrões como o PCI DSS (*Payment Card Industry Data Security Standard*) [PCI 2006].

Sabe-se que as empresas precisam implementar a gestão de risco de forma consistente e sistematizada. Porém, não há um *modelo de maturidade* voltado à Gestão de Riscos em Segurança da Informação que meça ou avalie o nível de maturidade desse processo dentro das organizações conforme os requisitos de um SGSI e, portanto, aplicável a empresas de diferentes portes e segmentos de mercado.

O objetivo (contribuição) principal deste artigo é especificar e estruturar um modelo para avaliar o nível de maturidade das empresas em relação ao processo de Gestão de Riscos em Segurança da Informação.

O objetivo específico é propor um instrumento (por exemplo, questionário ou lista de verificação) para auditoria de análise do nível de maturidade de uma instituição frente ao processo de gestão de riscos em Segurança da Informação.

O presente artigo apresenta-se organizado da seguinte maneira: a seção 2 apresenta o processo de gestão de risco; a seção 3 aborda alguns modelos de maturidade disponíveis no mercado; na seção 4 apresenta-se um esboço da proposta do Modelo para Avaliar o Nível de Maturidade do Processo de Gestão de Riscos em Segurança da Informação; e finalmente, a seção 5 encerra este artigo com algumas considerações parciais e trabalhos futuros.

2. Gestão de Riscos

Atualmente a *gestão de riscos* é um elemento central na gestão da estratégia de qualquer organização. O gerenciamento de riscos deve ser um processo contínuo e em constante desenvolvimento aplicado a estratégia da organização e à implementação desta estratégia. Deve analisar metodicamente todos os riscos inerentes às atividades passadas, presentes e futuras de uma organização e deve estar também integrada a cultura da organização com uma política eficaz e um programa conduzido pela alta

direção. O ponto central de um bom gerenciamento de riscos é a identificação e tratamento dos mesmos [Ferma 2003].

A norma AS/NZS 4360 [QSP 2004], utilizada na Austrália e Nova Zelândia, é uma das principais referências normativas sobre gestão de riscos disponíveis atualmente e serve como base para o desenvolvimento da ISO 31000, cujo objetivo é se tornar um conjunto único de diretrizes para a área e um modelo de gestão integrada do risco, de forma que possa ser utilizada por organizações de qualquer tipo, tamanho e segmento.

Segundo o QSP (2004), o processo de gestão de riscos compreende as etapas de: Estabelecimento dos contextos, Identificação de riscos, Análise de riscos, Avaliação de Riscos, Tratamento de Riscos, Comunicação e Consulta, e Monitoramento e Análise Crítica, detalhadas nas próximas seções.

2.1. Estabelecimento dos contextos

Estabelecimento do contexto significa definir o que fazer e como mensurar se estamos sendo bem sucedidos, a quem podemos causar impacto com nosso trabalho e quais as categorias ou grupos de atividades que compõem este trabalho [QSP 2004].

A fase de Estabelecimento dos Contextos envolve (1) definir responsabilidade para o processo de gestão de risco, (2) definir o escopo, (3) definir atividades, processos, funções, projeto, produto, serviço ou bens em termos de tempo e locação, como também seus objetivos e finalidades, (4) definir a metodologia do cálculo do risco, (5) definir a forma que o desempenho será avaliado no gerenciamento de risco, (6) identificar e especificar as decisões que devem ser tomadas e (7) identificar e colocar escopos e posicionar estudos necessários [ISO 2008]. Após a definição do escopo da gestão de riscos é realizada a identificação dos riscos nos processos.

2.2. Identificação de riscos

Identificação de riscos é o processo para localizar, listar e caracterizar elementos do risco, ou seja, é o processo que define aqueles eventos ou resultados que possam ter impacto para uma organização atingir o sucesso, deixando claro como, onde e por que o impacto pode acontecer [ABNT 2008].

É necessário identificar em cada processo de negócio: os Ativos, os Eventos (Vulnerabilidades, Ameaças e Danos/Conseqüências) e os Controles já existentes na empresa [ABNT 2005a]. Após a identificação dos riscos, é necessário considerar possíveis causas e cenários que mostram quais conseqüências que estes riscos podem trazer para a organização, considerando todas as causas significativas [ISO 2008]. Após a documentação destes dados, inicia a análise de cada um dos riscos identificados.

2.3. Análise de riscos

É o uso sistemático de informações para identificar fontes e estimar riscos, ou seja, é o processo que atribui valor ao impacto que um risco pode ter (conseqüência) e a probabilidade de sua ocorrência [ABNT 2005a].

O resultado desta análise é a identificação de todos os eventos, dos impactos desses eventos para cada propriedade da segurança da informação – confidencialidade,

integridade e disponibilidade (CID) -, as probabilidades de ocorrência, os impactos e o valor estimado dos riscos para cada evento/ativo [ABNT 2005a].

Segundo a ABNT (2008) as duas formas de estimativa de riscos são:

- **qualitativa:** utiliza uma escala com atributos qualificadores como, por exemplo, pequena, média e grande.
- **quantitativa:** utiliza uma escala de valores numéricos tanto para conseqüência quanto para a probabilidade.

Concluída a análise, se inicia a avaliação destes riscos.

2.4. Avaliação de Riscos

A avaliação determina a prioridade de cada risco através de uma comparação entre o nível estimado do risco determinado na análise e critérios pré-estabelecidos (nível de aceitação) para determinar a importância do risco [ABNT 2005]. Se o nível de risco não coincidir com o critério pré-estabelecido o risco deve ser tratado [ISO 2008]. No final da avaliação temos uma lista de riscos ordenados por prioridade e associados aos cenários de incidentes que os provocam. Assim, já se sabe quais os riscos que precisam ser tratados [ABNT 2008].

2.5. Tratamento de Riscos

Tratamento é a ação empreendida após a identificação, análise e a avaliação de riscos considerados inaceitáveis para a organização, ou seja, é o "processo de seleção e implementação de medidas (controles) para modificar um risco" [ABNT 2005a]. O tratamento envolve um processo cíclico de cálculo de um tratamento de risco, definindo se os níveis de riscos residuais[1] são toleráveis ou não, e se não toleráveis a geração de um novo tratamento de riscos e cálculo de efeitos daqueles tratamentos até que o risco residual atinja os critérios de risco estabelecidos pela organização [ISO 2008].

Segundo a ABNT (2008) as modificações possíveis através dos controles aplicados são:

- **Redução do risco:** ações tomadas para reduzir a probabilidade, as conseqüências negativas, ou ambas, associadas a um risco.
- **Retenção do risco:** aceitação do ônus da perda.
- **Evitar o risco:** a empresa decide pela eliminação de uma atividade planejada ou existente para evitar a ocorrência do risco.
- **Transferência do risco:** compartilhamento com outra entidade do ônus da perda ou do benefício do ganho associado a um risco.

Segundo a ISO (2008) o plano de tratamento de riscos deve incluir: (1) benefício esperado, (2) medidas de desempenho e restrições, (3) pessoas com que se pode contar, que são confiáveis para a aprovação e implementação do plano, (4) ações propostas, (5)

[1] Risco Residual é um novo valor (estimado) do risco após ter sido implementado controles que minimizam o impacto ou a probabilidade de o risco ocorrer.

o reporte e monitoramentos dos requerimentos, (6) os recursos necessários e (7) uma idéia de tempo e calendário para a implementação.

Ao término do tratamento todos os controles implementados estão cuidadosamente descritos, de forma que a identificação e os objetivos dos controles, bem como a identificação dos riscos (eventos) que o mesmo procura mitigar, a descrição desses controles, as métricas relacionadas e as metas dos mesmos sejam bem claras [ABNT 2005a].

2.6. Comunicação e Consulta

A comunicação consiste na troca ou compartilhamento de informação sobre o risco entre o tomador de decisão e as outras partes interessadas [ABNT 2008]. A organização deve criar um plano de comunicação e consulta entre ambos os *stakeholders*[2] internos e externos já nas etapas iniciais do gerenciamento de riscos, pois a comunicação e consulta deve acontecer em todas as etapas [ISO 2008].

2.7. Monitoramento e Análise Crítica

Monitoramento é o processo que tem como objetivo verificar, supervisionar, observar criteriosamente ou registrar a melhoria de uma atividade, ação ou sistema a fim de identificar mudanças após os tratamentos [ABNT 2005a]. O monitoramento constante e a análise crítica são necessários para assegurar que o contexto, o resultado da análise/avaliação de riscos e do tratamento do risco, assim como os planos de gestão, permaneçam relevantes e adequados às circunstâncias [ABNT 2008].

3. Modelos de Maturidade

Um modelo de maturidade funciona como um guia para a organização, de tal maneira que a empresa possa localizar onde está e como está “espelhando-se” nele para, em seguida, realizar um plano para que possa chegar à algum ponto melhor do que o atual, na busca da excelência. Atuam como referência para a obtenção de níveis adequados de qualidade nos bens e serviços produzidos ou utilizados nas relações comerciais, possibilitam uma linguagem comum, padronizam os bens e serviços e servem como apoio legal [Miyashiro 2007].

Considera-se que uma empresa atingiu sua maturidade quando os seus processos são explicitamente definidos, gerenciados, medidos, controlados e eficazes, ou seja, tem mecanismos que garantem a sua repetição sucessiva com bons resultados futuros relacionado, principalmente, à qualidade, custos e prazos [Siqueira 2005].

Na próxima seção é apresentada a proposta de um Modelo para Avaliar o Nível de Maturidade do Processo de Gestão de Riscos em Segurança da Informação e para a construção deste modelo foram estudados os modelos de maturidade: CMMI® (*Capability Maturity Model Integration*), COBIT® (*Control Objectives for Information and related Technology*), MMGP (Modelo de Maturidade em Gerencia de Projetos) e o OPM3 (*Organizational Project Management Maturity Model*).

[2] Termo em inglês que se refere a todos os interessados ou envolvidos no processo.

4. Proposta do Modelo

Baseado no estudo realizado sobre o processo de Gestão de Riscos (seção 2) e nos modelos de maturidade (seção 3) é apresentado a seguir a proposta de um Modelo para Avaliar o Nível de Maturidade do Processo de Gestão de Riscos em Segurança da Informação.

O modelo é constituído por um conjunto de boas práticas que oferece uma estrutura formal para o desenvolvimento da gestão de riscos de segurança da informação. O modelo é norteado por três estágios:

- **Imaturidade:** os processos da organização são improvisados ou não são seguidos.
- **Maturidade**: a organização já tem seus processos definidos, padronizados e controlados. Quanto mais madura a organização for, melhor e mais consistente é sua atuação.
- **Excelência:** a organização consegue otimizar seus processos, pois todos estão engajados em atividades de melhoria contínua. Tem-se uma evolução controlada de tecnologias e processos.

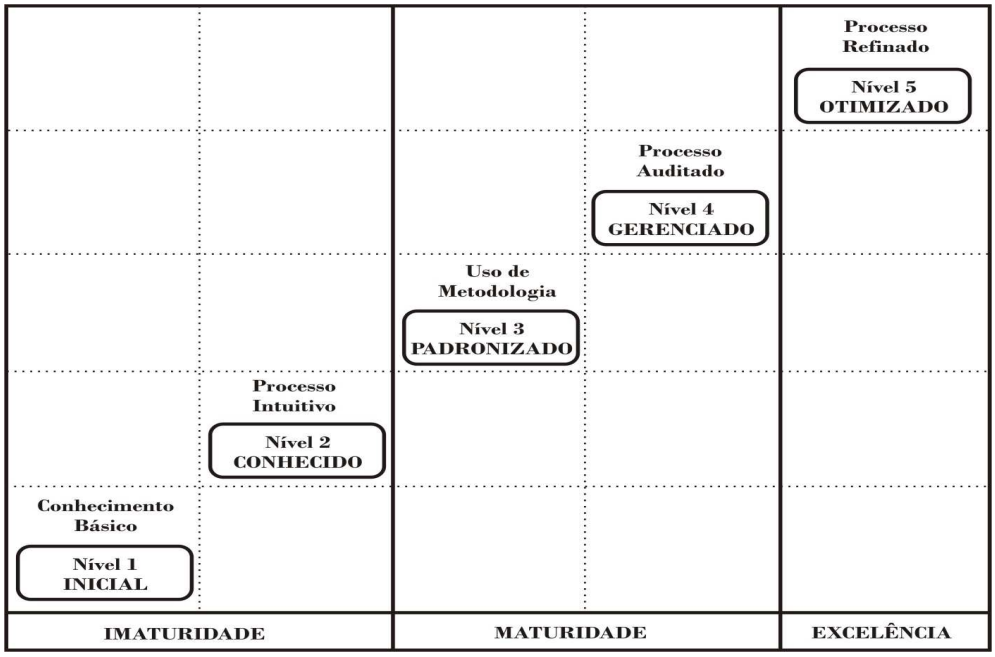

Figura 1. Proposta do Modelo para avaliar o nível de Maturidade do Processo de Gestão de Riscos em Segurança da Informação

O modelo consiste em cinco níveis de maturidade, conforme é ilustrado na Figura 1, para que a empresa alcance plena maturidade do gerenciamento de riscos em segurança da informação. Os cinco níveis são:

Nível 1 – Inicial: a empresa tem um conhecimento básico sobre o processo de gestão de riscos, porém ainda não o implementa.

Nível 2 – Conhecido: a organização tem um bom conhecimento sobre o processo de Gestão de riscos, porém apenas determinadas pessoas da área de segurança

da informação detêm esse bom conhecimento, que ainda não foi difundido por todo o setor. São essas as pessoas que realizam a gestão de riscos na empresa de forma dispersa e intuitiva, ou seja, nenhuma abordagem formal foi desenvolvida para a gestão de riscos.

Nível 3 – Padronizado: a empresa adotou um padrão para os processos de gestão de riscos com o uso de uma metodologia. Essa metodologia pode ter sido desenvolvida, com base na ISO 27005 [ABNT 2008], pela própria empresa, ou a empresa adotou uma metodologia já existente no mercado, como por exemplo, Octave (*Operationally Critical Threat, Asset, and Vulnerability Evaluation*) [Alberts e Dorofee 2001] e NIST SP 800-30 [Nist 2002].

A organização desenvolveu uma política de Gestão de Riscos, que está disponível a toda equipe de Segurança da Informação que recebeu treinamentos para sua utilização.

A empresa tem definido de forma sistemática como identificar fontes e estimar riscos, bem como estimar o valor do impacto e da probabilidade em função das escalas previamente definidas, seja de forma quantitativa ou qualitativa, e também pelo histórico da instituição. O critério de aceitação do risco, bem como o cálculo do Risco Residual, também estão bem definidos.

Nível 4 – Gerenciado: o processo de Gestão de Riscos da empresa é auditado e sua avaliação é utilizada pela direção para tomada de decisão. O conhecimento é amplo por parte de toda a equipe em relação ao processo de gestão de riscos e dos processos da área de Segurança da Informação.

É implementado um processo de Gerenciamento de Incidentes, o qual é baseado no ITIL® (*Information Technology Infrastructure Library*) [Miura 2007], que tem como foco principal restabelecer o serviço o mais rápido possível minimizando o impacto negativo no negócio, uma solução de contorno ou reparo rápido.

Nível 5 – Otimizado: a empresa atingiu um nível de excelência, pois consegue estimar de forma precisa os riscos, impactos e probabilidades de seus processos, assim elimina desperdícios, falhas e retrabalhos, conseguindo níveis elevados de eficácia.

A organização se torna mais efetiva no controle de desempenho e mais previsível, pois a diferença entre os resultados desejados e os resultados reais atingidos é quase nula. A empresa consegue refinar os seus processos e os controles do processo de gestão de riscos já estão incorporados às operações.

Cada etapa da Gestão de Riscos será avaliada e classificada em um nível de maturidade, conforme o modelo proposto. São utilizadas como base as seis etapas do processo de gestão de risco da norma ISO 27005[3] [ABNT 2008]: (1) definição de contexto, (2) análise/avaliação, (3) tratamento, (4) aceitação, (5) comunicação e (6) monitoramento e análise crítica dos riscos.

A Figura 2(a) representa uma empresa que alcançou o nível 4 de maturidade para a primeira etapa do processo, contudo em relação às demais etapas ainda encontra-se em

[3] O lançamento oficial dessa norma no Brasil está prevista para o inicio do segundo semestre deste ano.

um estágio de imaturidade. Já na Figura 2(b) foi representado um cenário[4] em que a empresa atingiu um nível de padronização em todas as atividades.

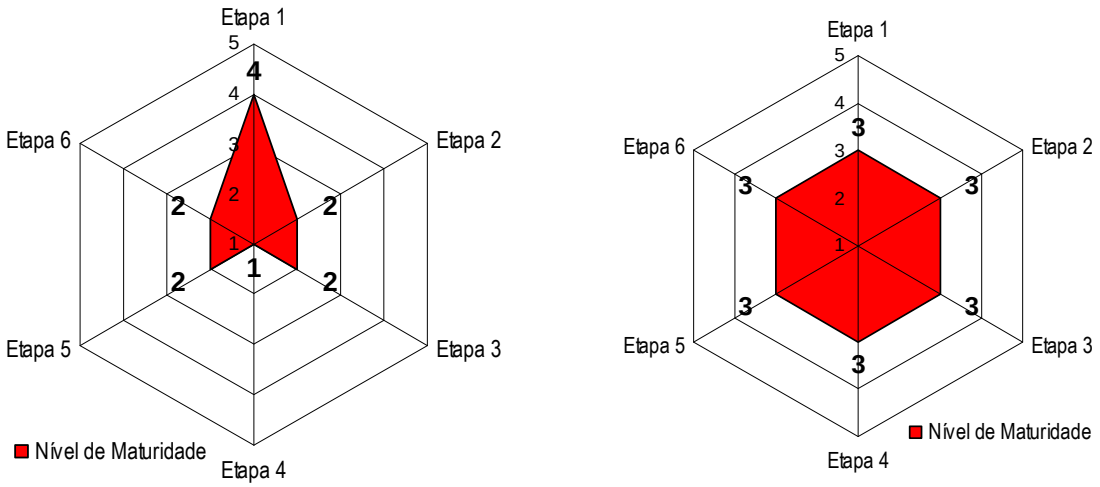

Figura 2. Nível de Maturidade por Etapa do Processo de GRSI

5. Considerações Finais

A gestão de riscos em segurança da informação é uma questão estratégica para as organizações e, portanto, esse processo deve ser constantemente melhorado e amplamente compreendido. Nesse contexto, o artigo em questão tem como objetivo especificar um Modelo para avaliar o nível de Maturidade das empresas em relação ao Processo de Gestão de Riscos em Segurança da Informação.

Os resultados da avaliação da maturidade do processo de gestão de riscos em Segurança da Informação fornecerão informações valiosas que podem ajudar a organização a planejar, executar e monitorar suas iniciativas de melhoria e gerenciamento de seus processos de negócios, bem como orientar os processos de tomada de decisão.

Ainda é necessário revisar e ampliar a descrição formal do Modelo de Maturidade do Processo de Gestão de Riscos em Segurança da Informação e concluir a elaboração de um instrumento de auditoria e avaliação dos níveis de maturidade que servirá de base para avaliar em que nível de maturidade se encontra uma determinada empresa. Por fim, esse instrumento será repassado a algumas instituições já definidas e os dados serão analisados.

Após a conclusão acredita-se que sejam trabalhos futuros pertinentes: (a) ampliar o número de estudos de caso com o objetivo de identificar necessidades de ajustes no modelo de maturidade, (b) aprimorar os instrumentos de avaliação e (c) desenvolver

[4] O nível de padronização representa que a empresa possui conformidade com os requisitos de gestão de riscos de um Sistema de Gestão da Segurança da Informação (SGSI).

uma ferramenta de apoio ao processo de avaliação e monitoramento dos níveis de maturidade.

Referências

ABNT – Associação Brasileira de Normas Técnicas (2005) "Norma NBR ISO/IEC 27001 - *Information Security Management Systems-Requirements*", Rio de Janeiro.

ABNT – Associação Brasileira de Normas Técnicas (2005a) "Norma NBR ISO/IEC Guia 73: Gestão de Riscos – Vocabulário –Recomendação para uso em normas", Rio de Janeiro.

ABNT – Associação Brasileira de Normas Técnicas (2008) "Norma NBR ISO/IEC 27005: Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação", Rio de Janeiro.

Alberts, C. e Dorofee, A. (2001) "*OCTAVE Criteria* v2.0", http://www.sei.cmu.edu, Janeiro.

BCB - Banco Central do Brasil (2006) "Resolução 3380/BACEN", http://www5.bcb.gov.br, Fevereiro.

BSI (2006) "BS 25999-1:2006: Código de Práticas para a Gestão da Continuidade do Negócio", Londres.

Chrissis, M. B., Konrad, M. e Shrum, S. (2005) "CMMI® - *Guidelines for Process Integration and Product Improvement*", Estados Unidos.

Ferma – *Federation of European Risk Management Associations* (2003), "Norma de Gestão de Riscos", Europa.

ISO – *International Organization for Standardization* (2008) "Norma ISO/DIS 31000: *Risk management – Principles and guidelines on implementation*", Suiça.

ITGI - *IT Governance Institute* (2007) "Cobit® 4.1", http://www.itgi.org, Maio.

Miura, G. S. (2007) "Estudo do Modelo ITIL e Avaliação das Gerências de Incidentes e Mudanças no contexto de um Processo de Negócio Real", https://www.icmc.usp.br/~estagio/computacao/monografias/glauciomiura.pdf, Janeiro.

Miyashiro, M. A. S. (2007) "Identificação e melhoria do nível de maturidade de uma organização explorando técnicas de inteligência computacional", INPE, São José dos Campos.

Módulo *Security* (2007) "10ª Pesquisa Nacional de Segurança da Informação", http://www.modulo.com.br/media/10a_pesquisa_nacional.pdf, Fevereiro.

NIST - *National Institute for Standards and Technology* (2002) "NIST SP 800-30", http://www.csrc.nist.gov, Junho.

PCI - *Payment Card Industry* (2006) "*Payment Card Industry (PCI) Data Security Standard v1.1*", https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf, Março.

PMI - *Project Management Institute* (2006) "PMI *Fact Sheet*", http://www.pmi.org, Maio.

Prado, D. (2006) “MMGP - Um modelo brasileiro de maturidade em gerenciamento de projetos”, http://pontogp.wordpress.com/2006/05/06/mmgp-um-modelo-brasileiro-de-maturidade-em-gerenciamento-de-projetos, Maio.

QSP – Centro da Qualidade, Segurança e Produtividade para o Brasil e América Latina (2004) “Gestão de Riscos – A norma AS/NZS 4360:2004”, *Risk* Tecnologia Editora, São Paulo.

Risk Bank (2002) “O Novo Acordo de Capital da Basiléia (Basiléia II)”, http://www.riskbank.com.br, Março.

Santos, L. de A. A. e Lemes, S. (2004) “A Lei Sarbanes-Oxley: uma tentativa de recuperar a credibilidade do mercado de capitais norte-americano”, Congresso EAC, São Paulo, http://www.congressoeac.locaweb.com.br, Março.

Santos, R. (2008) “O Bê-a-Bá da Gestão de Risco e Governança”, OTG, Brasília, http://www.otg.org.br, Fevereiro.

SEI - S*oftware Engineering Institute* (2008) “What is CMMI”, http://www.sei.cmu.edu/cmmi/general/index.html, Maio.

Sêmola, M. (2003) “Gestão da Segurança da Informação: uma visão executiva da segurança da informação: aplicada ao *security officer*”, Editora Campus, Rio de Janeiro.

Siqueira, J. (2005) “O Modelo de Maturidade de Processos: como maximizar o retorno dos investimentos em melhoria da qualidade e produtividade”, IBQN, Brasil, http://www.ibqn.com.br, Fevereiro.

Soler, A.o M. (2006) “Maturidade Organizacional e o Modelo de Avaliação PMI-OPM3”, J2DA *Consulting*, São Paulo, http://www.ieee.org/portal/site, Maio.

Swarowsky, H. H. e Deschamps, A. (2008) “CMMI – *Capability Maturity Model Integration*”, http://www.ieee.org/portal/site, Maio.