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

Janice Mayer[1], Leonardo Lemes Fagundes[1]

[1]Universidade do Vale do Rio dos Sinos (UNISINOS)
Av. Unisinos, 950 – CEP 93.022-000 – São Leopoldo – RS – Brasil
janice.mayer6@gmail.com, llemes@unisinos.br

Abstract. *The Risk Management (RM) process comprises coordinated activities aimed at guiding and controlling an organization as far as risks are concerned. These activities encompass the definition of the context of analysis, assessment, treatment, acceptance, as well as the communication and the monitoring of information security risks. Organizations should implement RM in a consistent, systematic manner in order to achieve compliance with current laws, standards and regulations, and also meet mandatory requirements for the certification of an Information Security Management System. However, in the context of information security, no reference was found in literature for a model to assess the maturity level of an RM process. In order to overcome this problem, this study describes the structure of a model for the assessment of the maturity level of the RM process in the realm of Information Security. The designed model basically consists of a set of best practices, totally aligned with standard ISO/IEC 27005 and comprised of: (1) three stages; (2) five maturity levels; (3) forty-three control objectives; (4) control map; (5) assessment perspective; (6) RACI Chart; (7) risk scorecard; and also a (8) assessment instrument.*

Resumo. *O processo de Gestão de Riscos (GR) compreende atividades[1] coordenadas para direcionar e controlar uma organização no que se refere a riscos, isso inclui a definição de contexto, análise, avaliação, tratamento, aceitação, comunicação e monitoramento dos riscos de segurança da informação. As organizações precisam implementar GR de forma consistente e sistemática, para buscar conformidades com leis, normas e regulamentações vigentes, bem como atender a requisitos obrigatórios para certificação de um Sistema de Gestão de Segurança da Informação. No entanto, não se identificou na literatura um modelo para avaliação do nível de maturidade desse processo no contexto de segurança da informação. Para contornar este problema neste trabalho descreve-se a estrutura de um modelo para avaliar o nível de maturidade do processo de GR em Segurança da Informação. O modelo desenvolvido consiste basicamente de um conjunto de boas práticas, totalmente alinhado a norma ISO/IEC 27005 e constituído por: (1) três estágios; (2) cinco níveis de maturidade; (3) quarenta e três objetivos de controles; (4) mapa de controles; (5) perspectiva de avaliação; (6) RACI Chart; (7) risk scorecard e, ainda, (8) instrumento de avaliação.*

[1] No contexto deste artigo o termo "atividade(s)" é usado no lugar do termo "subprocesso(s)", para um maior alinhamento com a norma ISO/IEC 27005 [8].

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, a indisponibilidade e o comprometimento da integridade da informação colocarem em risco a execução de processos de negócios vitais, que podem provocar diversos danos às instituições, por exemplo, perdas financeiras irreparáveis e o não cumprimento dos níveis de serviços acordados. 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 os ativos críticos protegidos [Módulo *Security* 2007]. Neste contexto, a gestão de riscos é essencial para que a empresa identifique ameaças e vulnerabilidades e mensure os impactos de um incidente de segurança da informação (SI).

O *risco* é a probabilidade de ameaças explorarem vulnerabilidades, gerando perdas de confidencialidade, integridade e/ou disponibilidade, causando, possivelmente, impactos (conseqüências) nos negócios. Já o processo de *Gestão de Riscos* (GR) compreende um conjunto de atividades coordenadas para direcionar e controlar uma organização no que se refere a riscos, incluindo definição de contexto, análise, avaliação, tratamento, aceitação, comunicação e monitoramento dos riscos [ABNT 2005].

No que tange a leis e regulamentações, cabe mencionar o esforço realizado por diversas instituições ao redor do mundo para atingir a conformidade, por exemplo, com (1) o *Acordo da Basiléia II*, que recomenda às instituições financeiras implementar a gestão de risco operacional [Risk Bank 2002]; e (2) a *Lei Sarbanes-Oxley*, promulgada pelo congresso americano em 2002 para regulamentação do mercado de capitais, que exige que as empresas implementem a GR para fornecer maior confiança ao investidor [Santos e Lemes 2004]. Além disso, existem resoluções internas como no Brasil, em que (3) o Banco Central por meio da resolução *3380/BACEN* determina que instituições financeiras e demais empresas autorizadas a funcionar por esse órgão, mantenham uma estrutura de gerenciamento do risco [BCB 2006]. No contexto específico da área de segurança da informação, a gestão de riscos trata-se de um requisito obrigatório para (4) a implementação de um *Sistema de Gestão de Segurança da Informação* (SGSI) [ABNT 2006] e (5) serve como insumo para a elaboração da *análise do impacto* nos negócios – etapa preliminar à criação das estratégias de contingência [BSI 2006].

Sabe-se que as empresas precisam implementar a GR de forma consistente e sistematizada. Porém, não há um modelo de maturidade voltado à GR em Segurança da Informação que meça ou avalie o nível de maturidade desse processo dentro das organizações conforme os requisitos de um SGSI. Diferentemente do que acontece com outras áreas que já possuem modelos como o *Capability Maturity Model Integration* (CMMI) e o *Control Objectives for Information and related Technology* (COBIT).

Embora a GR seja um processo estratégico e que auxilia as organizações a focar e direcionar investimentos para os pontos mais vulneráveis do negócio, uma pesquisa realizada no Brasil [Módulo *Security* 2007] mostra que 65% das empresas consultadas não têm um procedimento formalizado para a análise de riscos e 61% delas jamais realizou uma análise de riscos na área de Tecnologia da Informação (TI).

Um *modelo de maturidade* localiza as deficiências na estruturação e no gerenciamento dos processos e, conseqüentemente, as causas de desempenhos insatisfatórios. Provê bases e orientações para melhorias contínuas no processo, identificando e planejando objetivamente três tipos básicos de ações de melhoria: (1) previsibilidade, (2) controle e (3) eficácia [Siqueira 2005].

Este artigo propõe um modelo para avaliar o nível de maturidade do processo de GR em SI[2]. Este modelo define estágios e níveis de maturidade para o processo e está baseado em controles totalmente alinhados com a ISO/IEC 27005 [ISO 2008].

O presente artigo apresenta-se organizado da seguinte maneira: a seção 2 apresenta o processo de GR de SI; a seção 3 aborda os modelos de maturidade estudados, bem como apresenta a estrutura do Modelo para Avaliar o Nível de Maturidade do Processo de Gestão de Riscos em Segurança da Informação (MMGRseg); e finalmente, a seção 4 encerra este artigo com as conclusões.

2. Gestão de Riscos

Conforme ilustrado na Figura 1 o processo de gestão de riscos compreende as seguintes atividades: (1) definição de contexto, (2) análise/avaliação, (3) tratamento, (4) aceitação, (5) comunicação e (6) monitoramento e análise crítica dos riscos.

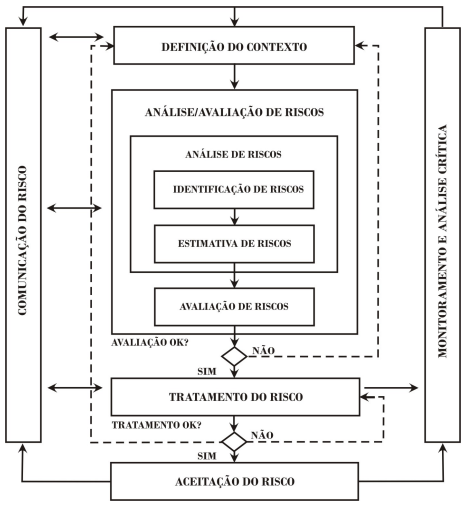

Figura 1. Processo de Gestão de Riscos, segundo a ISO/IEC 27005 [ISO 2008]

- **Definição de Contexto:** definir o que fazemos e como mensurar se estamos sendo bem sucedidos, a quais ativos e/ou organizações podemos causar impacto e quais as categorias de atividades que compõem este trabalho [QSP 2004].
- **Análise/Avaliação de Riscos:** convém que os riscos sejam identificados, quantificados ou descritos qualitativamente, priorizados em função dos critérios de avaliação de riscos e dos objetivos relevantes da organização [ISO 2008].
- **Tratamento de riscos:** é processo de seleção e implementação de medidas (controles) para modificar um risco [ABNT 2006].

[2] Este artigo trata exclusivamente de Gestão de Riscos em Segurança da Informação, para qual não se encontrou um modelo da maturidade nas referências. Diferentemente de Gestão de SI, para qual há referências a respeito de modelo maturidade.

- **Aceitação do Risco:** a decisão de aceitar os riscos deve ser tomada e formalmente registrada, juntamente com a responsabilidade pela decisão [ISO 2008].
- **Comunicação do risco:** troca ou compartilhamento de informação entre os *stakeholders*[3] [ISO 2008].
- **Monitoramento e Análise Crítica dos Riscos:** processo constante com o objetivo verificar, supervisionar, observar criteriosamente ou registrar a melhoria de uma atividade, ação ou sistema [ABNT 2006].

3. MMGRseg

Um modelo de maturidade funciona como um guia para a organização, de tal maneira que possa localizar onde e como está, *"espelhando-se"* nele [Miyashiro 2007]. Considera-se que uma empresa atingiu a maturidade em uma disciplina quando os seus processos são explicitamente definidos, gerenciados, medidos, controlados e eficazes [Siqueira 2005].

Baseado no estudo realizado sobre o processo de GR (seção 2) e no estudo dos Modelos de Maturidade CMMI [Chrissis, Konrad e Shrum 2005], COBIT [ITGI 2007], *Organizational Project Management Maturity Model* (OPM3) [PMI 2006] e *Information Security Management Maturity Model* (ISM3) [ISM3 2009], o Modelo para Avaliar o Nível de Maturidade do Processo de Gestão de Riscos em Segurança da Informação (MMGRseg).

O MMGRseg é constituído por um conjunto de requisitos e boas práticas, alinhado com a norma ISO/IEC 27005 [ISO 2008], que oferece uma estrutura formal para o desenvolvimento da gestão de riscos em SI. Esta estrutura é constituída por: (1) três estágios; (2) cinco níveis de maturidade; (3) quarenta e três objetivos de controles; (4) mapa de controles; (5) perspectiva de avaliação; (6) RACI *Chart*; (7) *risk scorecard* e (8) um instrumento para avaliação do nível de maturidade das atividades do processo de GR em SI.

Durante o processo de maturidade em que o modelo se propõe a desenvolver, a empresa passará por três estágios, os quais norteiam o modelo proposto:

- **imaturidade:** os processos da empresa são improvisados ou não são seguidos;
- **maturidade:** a organização já tem seus processos definidos, padronizados e controlados. Quanto mais madura 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.

Esses três estágios englobam um ou mais níveis de maturidade, conforme mostra a Figura 2.

[3] Termo utilizado para se referir a todos os interessados ou envolvidos no processo.

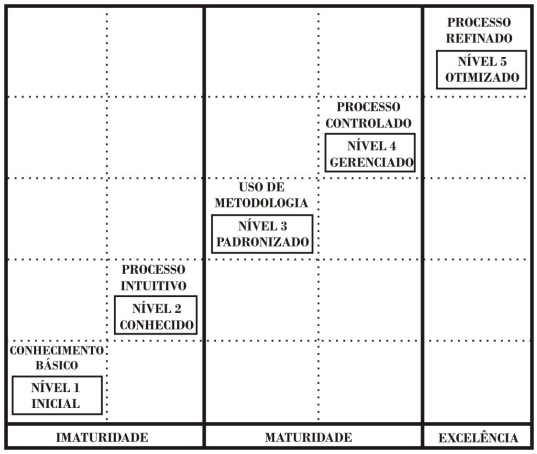

Figura 2. Modelo para avaliar o nível de Maturidade do Processo de Gestão de Riscos em Segurança da Informação (MMGRseg)

3.1. Níveis de Maturidade

Os *níveis de maturidade* representam um caminho para o processo de melhoria, indicando quais atividades devem ser implantadas para se alcançar cada nível, ilustrando assim a evolução da melhoria para toda a organização [SEI 2008]. A escolha do número de níveis do modelo MMGRseg e sua estrutura foram baseados nos modelos de maturidade estudados, em que pôde-se observar que a maioria dos modelos de maturidades seguindo uma lógica de um nível Informal, passando ao nível Organizado, Bem Estruturado, Gerenciado até chegar ao nível Otimizado.

O MMGRseg consiste em cinco níveis de maturidade, conforme é ilustrado na Figura 2, a fim de que a empresa alcance plena maturidade no processo de gerenciamento de riscos. Os níveis de maturidade representam uma maneira de controlar ou estruturar o desempenho da empresa, ou seja, é uma escala crescente de controle e visibilidade sobre o processo de GR em SI. Os cinco níveis do MMGRseg são:

- **Nível 1 – Inicial:** a empresa tem um conhecimento básico sobre determinada atividade do processo de gestão de riscos, porém ainda não o implementa.
- **Nível 2 – Conhecido:** a organização tem um bom conhecimento sobre determinada atividade do processo de GR, 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 atividade em questão de forma dispersa e intuitiva, ou seja, nenhuma abordagem formal foi desenvolvida para a atividade em questão do processo de GR.
- **Nível 3 – Padronizado:** a empresa adotou um padrão para a execução de determinada atividade do processo de GR com o uso de uma metodologia. Essa metodologia deve estar alinhada a ISO/IEC 27005 [ISO 2008].
- **Nível 4 – Gerenciado:** a atividade do processo de GR da empresa é auditada, ou seja, é feito um exame cuidadoso e sistemático, cujo objetivo é averiguar se as atividades estão de acordo com as disposições planejadas e/ou estabelecidas previamente, se foram implementadas com eficácia e se estão adequadas (em

conformidade) à consecução dos objetivos. O conhecimento é amplo por parte de toda a equipe em relação à atividade do processo de gestão de riscos de SI.

- **Nível 5 – Otimizado:** a atividade atingiu um nível de excelência, pois consegue eliminar desperdícios, falhas e retrabalhos, conseguindo níveis elevados de eficácia e a empresa transfere o conhecimento adquirido para ações futuras, conseguindo, assim, refinar o processo que envolve a atividade.

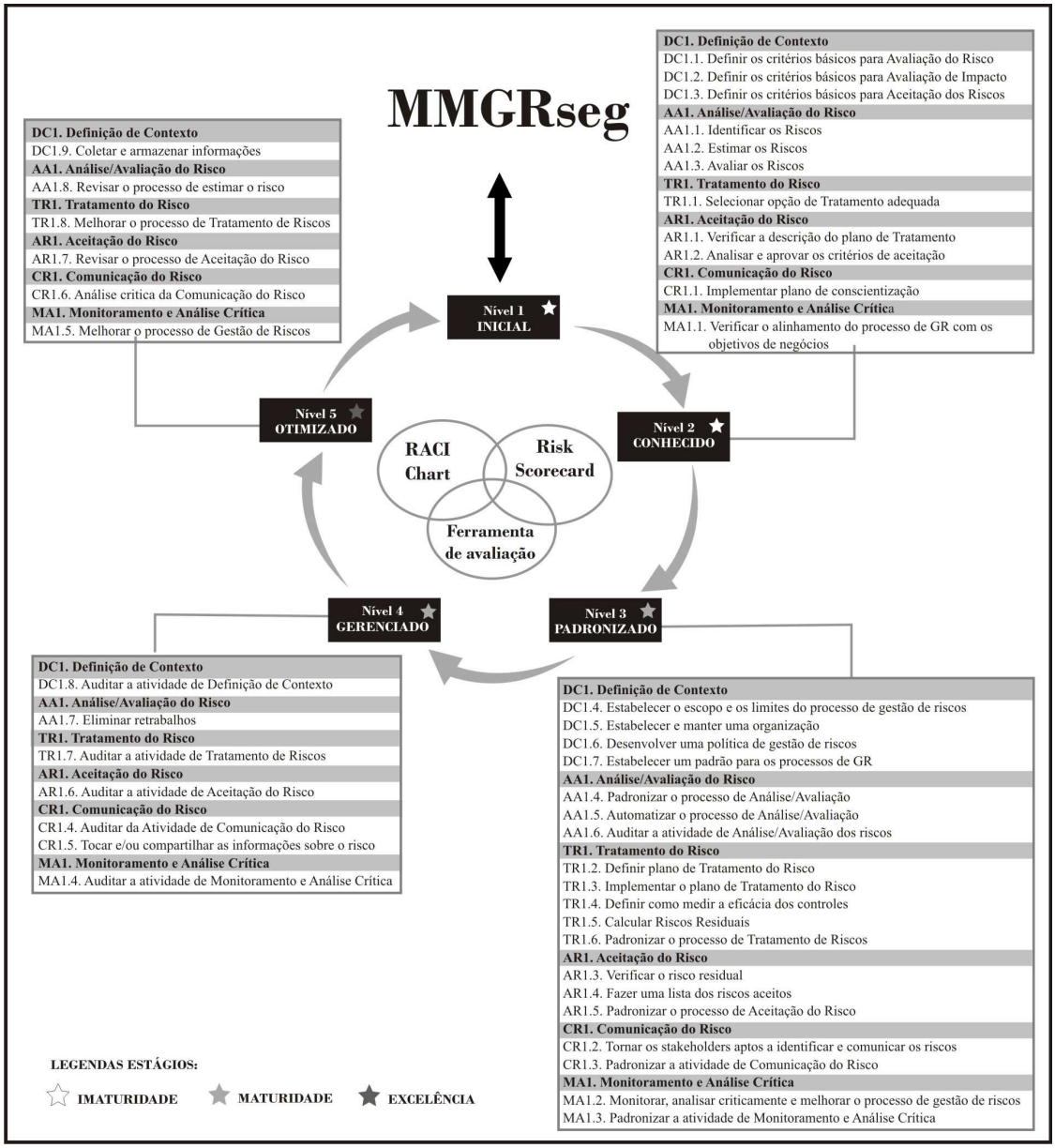

Figura 3. Estrutura do *framework* MMGRseg

O MMGRseg fornece orientações específicas para cada atividade do processo de GR em SI, listando o que deve ser trabalhado para atingir um nível de maturidade superior. Veja na Figura 3 a estrutura geral do *Framework* MMGRseg.

3.2. Objetivo de Controle

Um *objetivo de controle* é definido como uma declaração de um propósito ou resultado desejado a ser alcançado, por meio da implementação de controles em determinada atividade do processo de Gestão de Riscos em SI [ITGI 2007]. *Controles* são políticas, procedimentos, práticas e estruturas organizacionais, projetados para prover razoável garantia de que os objetivos de negócio serão alcançados e que eventos indesejáveis serão prevenidos, apagados ou corrigidos [ABNT 2005]. O MMGRseg define 43 objetivos de controle para as atividades do processo de GR apresentadas na seção 2, porém, os objetivos apenas serão citados a seguir, a descrição completa dos mesmos pode ser conferida em Mayer e Fagundes (2009).

DC1. Definição de Contexto

Os nove controles da atividade de Definição de Contexto são para definir o que fazer e como mensurar se está sendo bem sucedido, verificar a quais ativos e/ou organizações podemos estar causando impacto e quais as categorias ou grupos de atividades que compõem este artigo. Os controles são: DC1.1. Definir os critérios básicos para Avaliação do Risco; DC1.2. Definir os critérios básicos para Avaliação de Impacto; DC1.3. Definir os critérios básicos para Aceitação dos Riscos; DC1.4. Estabelecer o escopo e os limites do processo de gestão de riscos; DC1.5. Estabelecer e manter uma organização; DC1.6. Desenvolver uma política de gestão de riscos; DC1.7. Estabelecer um padrão para os processos de GR; DC1.8. Auditar a atividade de Definição de Contexto; e DC1.9. Coletar e armazenar informações.

AA1. Análise/Avaliação do Risco

Os controles da Análise/Avaliação do Risco são para identificar os riscos, quantificar ou descrever qualitativamente, priorizar em função dos critérios de avaliação de riscos e dos objetivos relevantes da organização. Os oito controles são: AA1.1. Identificar os Riscos; AA1.2. Estimar os Riscos; AA1.3. Avaliar os Riscos; AA1.4. Padronizar o processo de Análise/Avaliação; AA1.5. Automatizar o processo de Análise/Avaliação; AA1.6. Auditar a atividade de Análise/Avaliação dos riscos; AA1.7. Eliminar retrabalhos; e AA1.8. Revisar o processo de estimar o risco.

TR1. Tratamento do Risco

Os controles da atividade de Tratamento de Risco são para modificar os riscos. Os oito controles são: TR1.1. Selecionar opção de Tratamento adequada; TR1.2. Definir plano de Tratamento do Risco; TR1.3. Implementar o plano de Tratamento do Risco; TR1.4. Definir como medir a eficácia dos controles; TR1.5. Calcular Riscos Residuais; TR1.6. Padronizar o processo de Tratamento de Riscos; TR1.7. Auditar a atividade de Tratamento de Riscos; e TR1.8. Melhorar o processo de Tratamento de Riscos.

AR1. Aceitação do Risco

Os controles da Aceitação do Risco se referem à tomada de decisão da empresa de aceitar os riscos, que deve ser feito de maneira formal, guardando-se os devidos registros. Os sete controles são: AR1.1. Verificar a descrição do plano de Tratamento; AR1.2. Analisar e aprovar os critérios de aceitação; AR1.3. Verificar o risco residual; AR1.4. Fazer uma lista dos riscos aceitos; AR1.5. Padronizar o processo de Aceitação

do Risco; AR1.6. Auditar a atividade de Aceitação do Risco; e AR1.7. Revisar o processo de Aceitação do Risco.

CR1. Comunicação do Risco

Os controles da Comunicação do Risco são para acompanhar a troca e/ou compartilhamento de informação sobre o risco entre o tomador de decisão e as outras partes interessadas. Os seis controles são: CR1.1. Implementar plano de conscientização; CR1.2. Tornar os *stakeholders* aptos a identificar e comunicar os riscos; CR1.3. Padronizar a atividade de Comunicação do Risco; CR1.4. Auditar da Atividade de Comunicação do Risco; CR1.5. Tocar e/ou compartilhar as informações sobre o risco; e CR1.6. Análise critica da Comunicação do Risco.

MA1. Monitoramento e Análise Crítica

Os controles da atividade de Monitoramento de Análise Crítica dos Riscos são para verificar, supervisionar, observar criteriosamente e/ou registrar a melhoria de uma atividade, ação ou sistema a fim de identificar mudanças. Os cinco controles são: MA1.1. Verificar o alinhamento do processo de GR com os objetivos de negócios; MA1.2. Monitorar, analisar criticamente e melhorar o processo de gestão de riscos; MA1.3. Padronizar a atividade de Monitoramento e Análise Crítica; MA1.4. Auditar a atividade de Monitoramento e Análise Crítica; e MA1.5. Melhorar o processo de GR.

3.3. Mapa de controles

O mapa de controles fornecido pelo MMGRseg (veja na Tabela 1), auxilia os auditores e gerentes a manter controles suficientes para garantir o acompanhamento das iniciativas no processo de GR e recomendar a implementação de novas práticas, se necessário. Os controles são acumulativos, portanto, para atingir o nível 5 é necessário ter todos os controles do nível 1 ao nível 4 implementados, além dos controles para o nível 5.

Tabela 1. Mapa dos controles a serem implementados em cada Atividade por Nível de Maturidade

Atividades de GR	Níveis de Maturidade				
	Nível 1	Nível 2	Nível 3	Nível 4	Nível 5
Definição de contexto	-	DC1.1, DC1.2 e DC1.3	DC1.4, DC1.5, DC1.6 e DC1.7	DC1.8	DC1.9
Análise/Avaliação do Risco	-	AA1.1 e AA1.2	AA1.3, AA1.4 e AA1.5	AA1.6	AA1.7 e AA1.8
Tratamento do Risco	-	TR1.1	TR1.2, TR1.3, TR1.4, TR1.5 e TR1.6	TR1.7	TR1.8
Aceitação do Risco	-	AR1.1 e AR1.2	AR1.3, AR1.4 e AR1.5	AR1.6	AR1.7
Comunicação do Risco	-	CR1.1	CR1.2 e CR1.3	CR1.4 e CR1.5	CR1.6
Monitoramento e Análise Crítica do Risco	-	MA1.1	MA1.2 e MA1.3	MA1.4	MA1.5

3.4. Perspectiva de avaliação

Alguns modelos de maturidade possuem mais de uma representação, como é o caso do CMMI, que possui duas representações: por estágios e contínua [SEI 2008]. O modelo MMGRseg segue a representação contínua, em que cada atividade do processo de GR é avaliada individualmente, assim cada atividade pode atingir um nível de maturidade independente do nível atingido pelas demais atividades, com isso a empresa consegue verificar em qual das atividades precisa se focar mais. São utilizadas como base todas as atividades do processo de gestão de risco da norma ISO/IEC 27005 [ISO 2008].

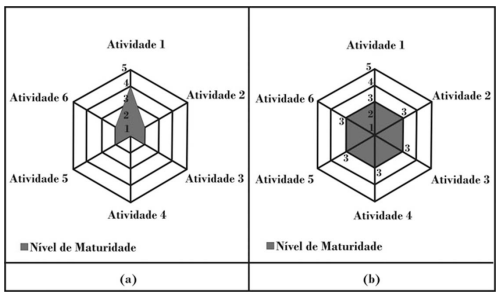

Figura 4. Dois exemplos de hipótese de avaliação do Nível de Maturidade por Atividade do Processo de Gestão de Riscos em Segurança da Informação

Como é apresentado no exemplo de hipótese da Figura 4, em que a Figura 4(a) representa uma empresa que alcançou o nível 4 de maturidade para a primeira atividade do processo, contudo em relação às demais atividades ainda encontra-se em um estágio de imaturidade. Já na Figura 4(b) foi representado um cenário[4] em que a empresa atingiu um nível de padronização em todas as atividades.

3.5. RACI Chart

Conforme Weill e Ross (2005) a especificação dos direitos decisórios e do *framework* de responsabilidades estimula comportamentos desejáveis. Isso significa que uma matriz de responsabilidades de decisões sobre o processo de gestão de riscos contribui para aumentar o comprometimento dos envolvidos e define claramente algumas das responsabilidades sobre as atividades do processo. Em Mayer e Fagundes (2009) é apresentada uma matriz de responsabilidades para os controles do MMGRseg, que foi elaborada usando o método RACI [ITGI 2008] com base nas informações sobre funções e atividades disponíveis no COBIT, mais especificamente no processo denominado *Assess and Manage IT Risks* e na norma ISO/IEC 27005 (2008).

3.6. Risk Scorecard

Segundo Kaplan e Norton (2001) todo processo deve ter objetivos e metas definidos para que seja possível medir o grau de sucesso na sua execução. Para tal, é necessário definir métricas conforme o modelo SMARRT (*Specific*, *Measurable*, *Actionable*, *Realistic*, *Results-oriented and Timely*). No modelo MMGRSeg todas as atividades do processo de gestão de riscos devem ser medidas com base nesse modelo.

[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).

Para a definição dos indicadores de desempenho é importante ter em mente que as atividades do processo de gestão de riscos possuem objetivos, esses objetivos devem ser medidos. Por exemplo, a atividade de tratamento de riscos possui como objetivo principal implementar controles para reduzir riscos, então indicadores como: tempo médio para implementação de controles e percentual de riscos identificados sem definição de uma estratégia de redução são chaves para o bom desempenho da atividade, pois de nada adianta identificar riscos rapidamente se a equipe responsável pela implementação dos controles não consegue implementá-los antes que ocorram os incidentes de segurança.

É importante que a relação de métricas e indicadores possa ser formulada por cada empresa. O risk scorecard não depende exatamente da organização, mas é algo flexível, pois talvez nem todas as métricas possam ser obtidas, dependendo do nível de maturidade da organização. Entretanto, o modelo proposto nesse artigo fornece um *risk scorecard* básico, que está em constante desenvolvimento e que deverá em médio prazo constituir uma base de indicadores que irá nortear todas as atividades.

3.7. Ferramenta de Avaliação

Foi elaborado um instrumento - em forma de questionário – que serve de base para as empresas avaliarem em que níveis de maturidade se encontram as atividades do processo de gestão de riscos em Segurança da Informação. O questionário utiliza a escala de *Likert* [Wainer 2006], para balancear respostas pré-definidas. A estrutura completa do questionário do modelo MMGRseg pode ser consultado em Mayer (2008).

Tabela 2. Relacionamento das perguntas do questionário com os níveis de maturidade e as atividades do processo de Gestão de Riscos em SI

	Definição de Contexto	Análise/ Avaliação do Risco	Tratamento do Risco	Aceitação do Risco	Comunicação do Risco	Monitoramento e Análise Crítica
Nível 2	Q3	Q9	Q15	Q21	Q26	Q31
Nível 3	Q4, Q5, Q6	Q10, Q11, Q12	Q16, Q17, Q18	Q22, Q23	Q27, Q28	Q32, Q33
Nível 4	Q7	Q13	Q19	Q24	Q29	Q34
Nível 5	Q8	Q14	Q20	Q25	Q30	Q35

O questionário é composto de 35 perguntas, das quais 1 e 2 são questões gerais para avaliar o Nível 1 de maturidade de todas as atividades do processo de Gestão de Riscos e SI, as demais questões estão relacionadas com os demais níveis de maturidade e com as atividades do processo de Gestão de Riscos em SI conforme mostra a Tabela 2.

4. Conclusão

A gestão de riscos em segurança da informação se tornou uma questão estratégica para as organizações, em função das exigências do mercado, do governo, de agências reguladoras e também dos clientes e, portanto, esse processo deve ser constantemente melhorado e amplamente compreendido. Nesse contexto, o MMGRseg é uma contribuição significativa para o amadurecimento da área de segurança da informação, pois organiza práticas efetivas em uma estrutura para estabelecer prioridades.

O MMGRseg é um modelo de maturidade composto por (1) três estágios; (2) cinco níveis de maturidade; (3) quarenta e três objetivos de controles; (4) mapa de controles; (5) perspectiva de avaliação; (6) RACI Chart em relação a cada uma das atividades do processo de GR; (7) um risk scorecard e, ainda, (8) um instrumento para avaliação do nível de maturidade das atividades do processo de GR.

O MMGRseg mostra onde a organização precisa focar esforços e investimentos para conseguir atingir a maturidade e, posteriormente, a excelência. Os resultados da avaliação com o MMGRseg ajudam a organização a planejar, executar e monitorar suas iniciativas de melhoria e gerenciamento de seus processos de negócios, melhorando assim, a previsibilidade dos resultados, o controle de seu desempenho e a eficácia. O MMGRseg é um modelo de maturidade único no que diz respeito a Gestão de Riscos em SI e está alinhado com a ISO/IEC 27005 (2008).

O MMGRseg pode ser utilizado pela organização para: (1) identificar os pontos fracos e/ou deficiências e as possibilidades de melhorias no processo, direcionando os investimentos em SI; (2) disseminar a cultura de GR por toda a empresa; (3) fazer um *benchmarking* de segmento, conseguindo comparar o nível de maturidade de cada atividade da empresa com outras organizações, o que possibilita troca de informações e amadurecimento; (4) atingir a eficácia no processo de melhoria contínua da GR em SI; e (5) orientar em projetos de certificação de SGSI e de Continuidade de Negócios.

Acredita-se que sejam trabalhos futuros pertinentes: (1) desenvolver uma versão *"light"* para o questionário; (2) aprimorar o modelo incluindo a representação por estágios, levando em conta o processo de GR como um todo; (3) realizar uma validação estatística do questionário; (4) definir métricas e indicadores para todas as atividades de gestão de riscos; (5) avaliação do modelo com especialistas de segurança da informação; e (6) um estudo de caso prático com a utilização do modelo. O estudo de caso com o MMGRseg já está programado e deverá ser concluído em agosto de 2010.

Referências

Associação Brasileira de Normas Técnicas (ABNT) (2005) "Código de Prática para a Gestão da Segurança da Informação: NBR ISO/IEC 27002", Rio de Janeiro: ABNT.

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

Banco Central do Brasil (BCB) (2006), "Resolução 3380/BACEN", Brasil: BCB, 2006. Disponível em: <http://www5.bcb.gov.br>. Acesso em: 23 de fev. de 2008.

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

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

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

International Organization for Standardization (ISO) (2008) "Information technology - Security techniques - Information security risk management: ISO/IEC 27005", Suiça.

ISM3 Consortium (2009) “ISM3: Information Security Management Maturity Model”, disponível em: <http://ism3.wordpress.com/2009/04/02/ism3-v23-published/>, acesso em: 05 jan. 2010.

IT Governance Institute (ITGI) (2007) “Cobit® 4.1”, USA: ITGI.

Kaplan, R. S. e Norton, D. P. (2001) “The Strategy-Focused Organization: How Balanced Scorecard Companies Thrive in the New Business Environment”, Boston, MA: Harvard Business School Press.

Mayer, Janice (2008) “Um Modelo para Avaliar o Nível de Maturidade do Processo de Gestão de Riscos em Segurança da Informação”, Brasil: monografia apresentada à Universidade do Vale do Rio dos Sinos (UNISINOS), São Leopoldo, diponível em: <http://www.fepal.com.br/TCC_JaniceMayer.rar>.

Mayer, J. e Fagundes, L.L. (2009) “A Model to Assess the Maturity Level of the Risk Management Process in Information Security”, in: 4th IEEE/IFIP International Workshop on Business-driven IT Management (BDIM), NY, USA, diponível em: <http://ieeexplore.ieee.org/Xplore/login.jsp?url=http%3A%2F%2Fieeexplore.ieee.org%2Fiel5%2F5174549%2F5195925%2F05195935.pdf%3Farnumber%3D5195935&authDecision=-203>.

Miyashiro, M. A. S. (2007) “Identificação e melhoria do nível de maturidade de uma organização explorando técnicas de inteligência computacional”, São José dos Campos: INPE (Instituto Nacional de Pesquisas Espaciais).

Módulo Security (2007) “10ª Pesquisa Nacional de Segurança da Informação”, São Paulo, disponível em: <http://www.modulo.com.br/media/10a_pesquisa_nacional.pdf >, acesso em: 23 de fev. de 2008.

Project Management Institute (PMI) (2006), “PMI Fact Sheet”, USA: PMI, 2006, disponível em: <http://www.pmi.org>, acesso em 10 mai. 2008.

Risk Bank (2002) “O Novo Acordo de Capital da Basiléia (Basiléia II)”, Rio de Janeiro: Risk Bank, 2002, disponível em: <http://www.riskbank.com.br/>, acesso em: 1º de mar. de 2008.

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

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

Siqueira, J. (2005) “O Modelo de Maturidade de Processos: como maximizar o retorno dos investimentos em melhoria da qualidade e produtividade”, Brasil: IBQN, 2005, disponível em: <http://www.ibqn.com.br>, acesso em: 28 de fev. de 2008.

Software Engineering Institute (SEI) (2008), “What is CMMI”, Pittsburgh: SEI, disponível em: <http://www.sei.cmu.edu/cmmi/general/index.html>, acesso em: 10 mai. 2008.

Wainer, J. (2006) “Métodos de pesquisa quantitativa e qualitativa para a Ciência da Computação”, São Paulo: Instituto de Computação – UNICAMP.