Avaliação de maturidade de processos de gestão de riscos de TI: ferramenta de apoio para a qualidade e eficiência do processo

Misael Sousa de Araújo[1]
Edgard Costa Oliveira[2]
Simone Borges Simão Monteiro[3]

Resumo: A tecnologia da informação possui papel fundamental nas organizações, figurando como um componente estratégico para seus processos de negócio. A aplicação da gestão de riscos no contexto da governança de TI é fator crítico de sucesso para o alcance dos objetivos estratégicos das organizações. No entanto, apenas adotar práticas de gestão de riscos não é suficiente para garantir que sua aplicação trará os resultados esperados. Cada vez mais as organizações têm buscado conhecer quão eficientes tem sido seus processos, incluindo o processo de gestão de riscos, de forma a conhecer seu grau de eficiência em uma determinada escala, conhecer suas deficiências, e assim traçar planos para melhoria de seus processos e ainda comparar seu desempenho em relação a organizações similares. Dado à diversidade de modelos de maturidade e suas características, este artigo realizou um estudo comparativo entre os principais modelos de maturidade do mercado, selecionou um modelo aplicado à gestão de riscos de tecnologia da informação (escolhida via técnica de decisão multicritério Analytic Hierarchy Process – AHP) e propôs um instrumento de avaliação de maturidade em gestão de riscos de TI que possa ser utilizado por qualquer organização.

Palavras-chave: Gestão de Risco. Governança de TI. Modelo de maturidade.

Abstract: *Information technology has a key role in the organizations, acting as an strategic component in their business processes. The use of risk management in the context of IT Governane is a critical success factor towards reaching the organization´s strategic goals. However, the adoption of risk management alone is not enough to garantee that its application will bring expected results. More and more organizations have searched for knowledge of how efficient their processes have been developed, including risk management processes. This is how they get to know their efficiency level in a determined scale, by knowing their deficiencies and thus making new plans to embetter their processes and to compare their performance in relation to other similar organizations. Due to the diversity of existing maturity models and their characteristics, this article presents the results of a comparative study with the main maturity models in the market, by selecting a specific one that can be applied to IT risk management processes, chosen via the application of AHP technique – Analytic Hierarchy Process – and as then proposes an instrument that can be used for the evaluation of IT risk management maturity. We believe that this instrument can be of general used by any organization.*

***Keywords**: Risk management. IT Governance. Maturity Model.*

[1] Coordenação de Gestão de Tecnologia da Informação e Comunicação – Fundação Oswaldo Cruz (Fiocruz) – Rio de Janeiro – RJ – Brasil
{misael.araujo@fiocruz.br}
[2] Departamento de Engenharia Elétrica –Universidade de Brasília (UnB) – Brasília – DF – Brasil
{ecosta@unb.br}
[3] Departamento de Engenharia de Produção –Universidade de Brasília (UnB) – Brasília – DF – Brasil
{simoneborges@unb.br}

http://dx.doi.org/10.5335/rbca.v9i2.6099

1. Introdução

As organizações têm se utilizado da potencialidade das tecnologias de informação para prestar seus serviços, onde as informações e as tecnologias que as suportam são considerados os seus bens mais valiosos. Para essas organizações, conhecer e gerenciar os riscos de TI associados aos seus ativos se torna uma atividade vital, pois disso dependem os processos de negócios críticos da organização. Segundo o IT Governance Institute [1], organizações bem-sucedidas entendem e gerenciam os riscos em seus processos de governança de TI. O Instituto Brasileiro de Governança Corporativa [2] recomenda que as organizações adotem um sistema de gerenciamento e controle dos riscos corporativos, como forma preventiva de conhecer os principais riscos, suas probabilidades de ocorrência, seus impactos e medidas de prevenção e mitigação que podem ser adotadas. Para Weill & Ross [3] a gestão de riscos é elemento chave da governança, onde uma governança mal concebida pode acarretar gastos desnecessários, aumento de despesas, interrupção das operações e iniciativas insuficientes à melhoria do desempenho organizacional.

Assim, a gestão de riscos de TI pode ser entendida como fator crítico de sucesso para que uma organização atinja seus objetivos. No entanto, somente isto não é suficiente. Faz-se necessário conhecer o quão eficiente está sendo implementado o processo de gestão de riscos em uma organização. A essa eficiência do processo de gestão de riscos, chamemos de maturidade em gestão de riscos. A norma ISO/IEC 15504-1 [4] recomenda a adoção de um processo de avaliação da capacidade afim de permitir a geração de uma pontuação para o processo e permitir a comparação entre organizações, independentemente de seu tamanho. Hopkinson [5] diz que uma transformação significativa da capacidade de gestão de riscos em uma organização é demorada, demandando esforço e tempo. Assim, a avaliação do nível de maturidade do processo de gestão de riscos se faz necessário não só para compreensão da sua situação atual, mas também para seu contínuo aperfeiçoamento.

Embora se identifique a adoção de práticas de gestão de riscos nas organizações, não se observa com a mesma frequência a implementação de métodos para aferição da maturidade das suas práticas em gestão de riscos. Shahzad e Safvi [6] afirmam que "organizações que tem alcançado um nível de maturidade mais elevado podem melhor evitar riscos em suas fases iniciais". Assim, é possível identificar alguns problemas associados à escolha de um modelo de maturidade em gestão de riscos, tais como:

- Desconhecimento de critérios que orientem a escolha de um modelo de maturidade que possa ser aplicado à gestão de riscos de TI;
- Variedade de modelos de maturidade existentes, não alinhados entre si, dificultando uma escolha;
- Ausência de instrumentos adequados à coleta de dados e avaliação prática do nível de maturidade em gestão de riscos de TI.

Como forma de responder e solucionar os problemas acima descritos, esse artigo apresenta uma proposta de solução para avaliação de maturidade de gestão de riscos de TI, a partir da escolha de um modelo de maturidade e definição de instrumento de avaliação. Para isso, os seguintes métodos foram adotados:

- Estudo comparativo entre modelos de maturidade existentes, tais como: frameworks, modelos acadêmicos e normas de referência, a fim de permitir uma rápida visão sobre suas principais características e subsidiar a escolha de um modelo;
- Seleção de um modelo de maturidade, dentre os diversos modelos existentes, capaz de atender adequadamente ao propósito da gestão de riscos de TI, a partir da adoção de um método específico e com base em critérios comuns;
- Desenvolvimento de um instrumento de coleta e avaliação de maturidade em gestão de riscos de TI, com base no modelo selecionado.

Este artigo está estruturado de forma a apresentar os principais conceitos necessários ao entendimento do tema, seguido de uma discussão metodológica e apresentação dos resultados alcançados.

2. Revisão teórica

Neste tópico são descritos os principais conceitos sobre o tema, apresentando os diferentes aspectos conceituais (mas não contraditórios) sobre os principais autores e a forma como se complementam.

2.1 Risco

Na literatura são encontradas diversas definições sobre risco, porém o entendimento sobre seu significado pode variar para cada indivíduo. O dicionário Aurélio define risco como "perigo ou possibilidade de perigo" ou ainda "situação em que há probabilidades mais ou menos previsíveis de perda ou ganho" [7]. A norma *ISO Guia 73* define o termo risco como "o efeito da incerteza nos objetivos" [8]. Essas incertezas não devem ser entendidas necessariamente como algo negativo, ao contrário, podem ser positivas e devem ser vistas como uma oportunidade a ser trabalhada em favor da organização para alcance de seus objetivos. Segundo o Instituto Brasileiro de Governança Corporativa – IBGC, "costuma-se entender 'risco' como possibilidade de 'algo não dar certo', mas seu conceito atual envolve a quantificação e qualificação da incerteza, tanto no que diz respeito às 'perdas' como aos 'ganhos'" [2]. Segundo o The Orange Book [9], risco é definido como uma incerteza do resultado de ações e eventos, seja uma oportunidade (positivo) ou uma ameaça (negativo).

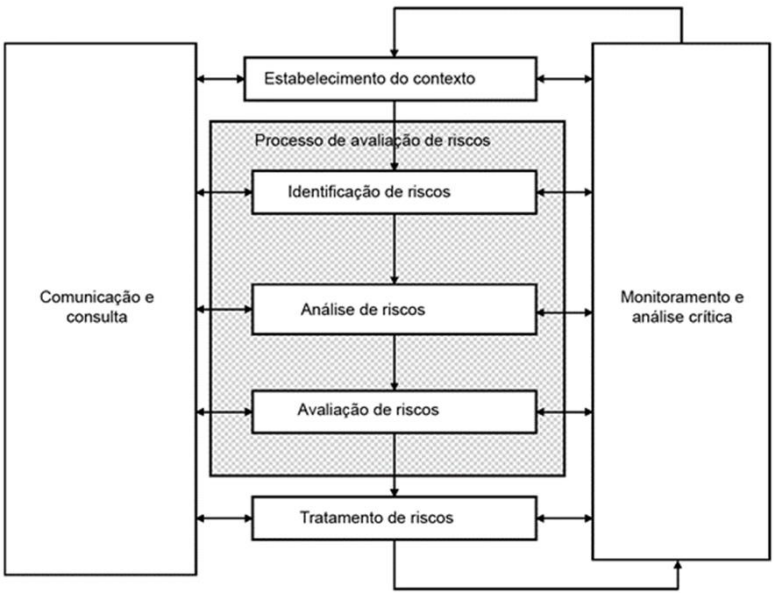
2.2 Gestão de riscos

O termo gestão de riscos está associado ao conjunto de atividades necessárias ao gerenciamento dos riscos. Segundo a norma ISO Guia 73 [8], que define o vocabulário para a gestão de riscos, o termo gestão de riscos pode ser entendido como "atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos". Para Elmaallam & Kriouile [10], a gestão de riscos é uma disciplina indispensável para qualquer organização no alcance de seus objetivos. Ramos define gestão de riscos como "o processo que identifica e trata os riscos de forma sistemática e contínua" [11]. Silveira [12] ressalta que a gestão de riscos é uma das funções primordiais dos conselhos de administração dentro de um processo de governança corporativa. É possível encontrar diversas descrições para o termo gestão de riscos, porém, todas traduzem de forma similar o seu significado. Para o SEI [13] a gestão de riscos é "um processo contínuo de antecipação de problemas, sendo uma parte importante da gestão que é aplicada durante toda a vida de um projeto para antecipar e mitigar, de forma efetiva, os riscos com impactos críticos no projeto". Para o DSIC [14] a gestão de riscos se refere ao "conjunto de processos que permitem identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos". Para o COSO [15] a gestão de riscos é um processo aplicado no estabelecimento de estratégias, formuladas para identificar em toda a organização eventos em potencial, capazes de afetá-la, e administrar os riscos de modo a mantê-los compatível com o apetite a risco da organização e possibilitar garantia razoável do cumprimento dos seus objetivos [15].

2.3 Processo de gestão de riscos

O processo de gestão de riscos, segundo a norma ISO 31000, consiste na "aplicação sistemática de políticas, procedimentos e práticas de gestão para as atividades de comunicação, consulta, estabelecimento do contexto, e na identificação, análise, avaliação, tratamento, monitoramento e análise crítica dos riscos" [16]. Ainda segundo a norma, o processo de gestão de riscos é composto da atividade de estabelecimento do contexto, de avaliação de riscos, tratamento de riscos, monitoramento e análise crítica e comunicação e consulta.

Figura 1: Processo de Gestão de Riscos [16]



O processo de avaliação do risco é subdivido em três outras atividades: identificação de riscos, análise de riscos e avaliação de riscos. Já as atividades de monitoramento e análise crítica e comunicação e consulta acontecem iterativamente durante todo o ciclo do processo de gestão de riscos.

2.4 Governança Corporativa e Governança de TI

De uma forma geral, observa-se que a gestão de riscos vem sendo adotada pelas organizações em seus processos de governança corporativa. Para o Instituto Brasileiro de Governança Corporativa – IBGC a Governança Corporativa é definida como o sistema pelo qual as organizações são dirigidas, monitoradas e incentivadas [2]. Para Silveira [12], governança corporativa é definida como o conjunto de mecanismos que visam fazer com que as decisões corporativas sejam sempre tomadas com a finalidade de se maximizar a perspectiva de geração de valor de longo prazo para o negócio. Segundo a Organização para a Cooperação e o Desenvolvimento Econômico, a governança corporativa "fornece a estrutura através da qual os objetivos da organização são definidos, e os meios para alcançar os objetivos e o desempenho de monitoramento são determinados" [17]. A Norma ISO/IEC 38500, por sua vez, define governança como "o sistema pelo qual as organizações são dirigidas e controladas" [18]. O conceito de governança de TI em nada difere dos conceitos de governança apresentados até aqui, pois os princípios são os mesmos: estrutura para decisão, monitoramento, responsabilização, etc. Weill & Ross [3] definem a governança de TI como a "especificação dos direitos decisórios e do *framework* de responsabilidades para estimular comportamentos desejáveis na utilização da TI". Os mesmos autores ressaltam ainda a importância da governança de TI nas organizações, onde afirmam que "uma boa Governança de TI harmoniza decisões sobre a administração e a utilização da TI com comportamentos desejáveis e objetivos do negócio" [3]

3. Metodologia

Para identificação e seleção dos modelos de maturidade existentes, foram realizadas entrevistas junto a especialistas da área, pesquisas documentais e bibliográficas e análise de conteúdo. Para a definição dos critérios a serem utilizados na escolha do modelo de maturidade, foram realizadas entrevistas estruturadas e aplicados questionários. Embora a lista de critérios obtida pelas entrevistas e questionários representem a opinião de especialistas, a lista poderia sofrer influência de tendências/preferências dos entrevistados por um determinado modelo. Assim, foi aplicada a técnica Delphi para obter um consenso confiável de opiniões do grupo de especialistas. Uma vez definidos os critérios, eles foram submetidos a uma medida de opinião. Considerando-se que as opiniões são baseadas em critérios tangíveis e intangíveis, arbitrariamente escolhidos por quem toma a decisão [19], foi empregada a técnica de decisão multicritério AHP – Analytic Hierarchy Process – um dos principais modelos matemáticos para apoio à teoria de decisão disponíveis no mercado [20]. Com base no

modelo de maturidade escolhido, foi desenvolvido um formulário para coleta de dados e avaliação do nível de maturidade que pudesse ser aplicado ao processo de gestão de riscos de tecnologia da informação.

4. Apresentação dos dados e análise dos resultados

4.1 Análise comparativa dos modelos de maturidade

Para compor a análise comparativa foram utilizados cinco modelos de maturidade, encontrados em frameworks de mercado, propostas acadêmicas e norma de referência. São eles: Capability Maturity Model Integration (CMMI) 1.3, Control Objectives for Information and related Technology (COBIT) 4.1, Formação de Valor em Sistemas de Atividades Humanas (FVSAH), norma ISO/IEC 15504 e Risk Maturity Model (RMM). Foram extraídas características comuns aos modelos estudados, agrupadas em cinco diferentes eixos: estrutura, concepção, robustez, flexibilidade e custos. Com base nessas informações, foi construída uma matriz, que apresenta de forma sintética as principais características dos modelos, representada pela tabela 1.

O conjunto de critérios apresentados serviram de insumo para a próxima fase do estudo (seleção do modelo), onde um conjunto de cinco especialistas – oriundos dos setores público e privado, com ampla experiência em governança e gestão de riscos – julgou a relevância dos critérios para escolha de um modelo de maturidade no contexto da gestão de riscos de TI.

5. Seleção do Modelo de Maturidade

Para a seleção do modelo de maturidade, foram identificados, inicialmente, um conjunto 23 critérios que, na opinião dos especialistas, deveriam ser considerados para a escolha do modelo. Para obter o consenso confiável de opiniões do grupo de especialistas foi utilizada a técnica Delphi, que permitiu definir com clareza quais critérios o grupo de especialistas tinha consenso sobre sua utilização, sendo assim reduzidos a 13 critérios.

5.1 Estrutura hierárquica de critérios para aplicação da técnica AHP

Para apoiar a escolha do modelo de maturidade, foi utilizada a técnica de decisão multicritério Analytic Hierarchy Process (AHP). Como a técnica exige a definição de uma estrutura hierárquica dos critérios, os treze critérios identificados foram agrupados em cinco categorias (estrutura, concepção, robustez, flexibilidade e custos).

Figura 2: Estrutura hierárquica de critérios utilizados para a avaliação dos modelos de maturidade

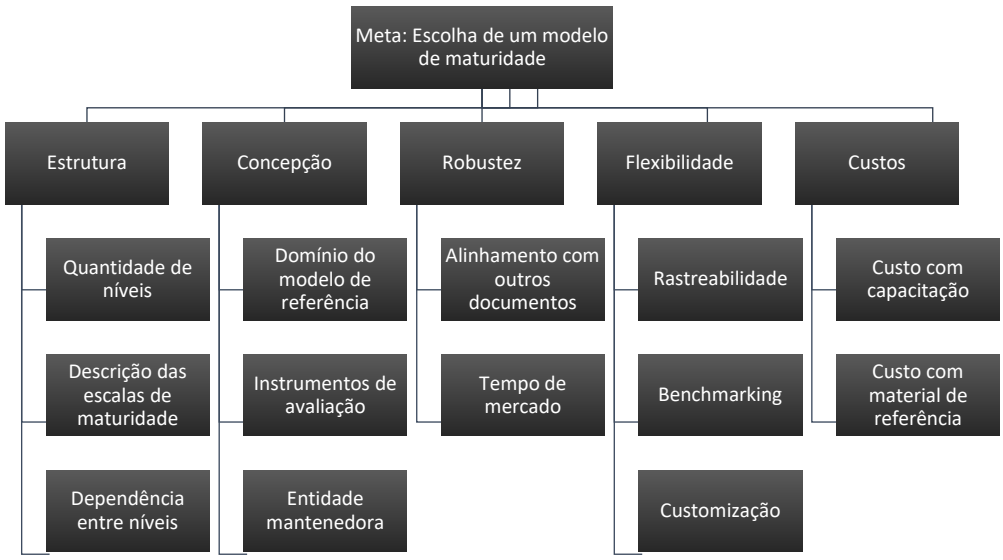


Tabela 1: Tabela comparativa dos modelos de maturidade aplicáveis à gestão de riscos de TI

Agrupamento	Características	CMMI 1.3	COBIT 4.1	FVSAH	ISO/IEC 15504	RMM
Estrutura	Quantidade de níveis	5	6	5	6	4
	Descrição das escalas de maturidade	Inicial - Gerenciado - Definido - Gerenciado quantitativamente – Em otimização	Incompleto - Executado - Gerenciado - Estabelecido - Previsível - Em otimização	Funcionamento - Especialização - Crescimento - Convergência - Referência	Incompleto - Executado - Gerenciado - Estabelecido - Previsível - Em otimização	Ingênuo - Principiante - Normalizado - Natural
	Dependência entre níveis	Sim	Sim	Sim	Sim	Não
Concepção	Domínio do modelo de referência	Engenharia de Software	Controle e Gerenciamento de TI	Genérico	Genérico	Gerenciamento de Risco
	Instrumentos de avaliação	Não	Sim	Não	Não	Não
	Entidade mantenedora	SEI	ISACA	Acadêmico [21]	ISO	Acadêmico [22]
Robustez	Alinhamento com outros instrumentos	CMM for SW, INCOSE SECAM e EIA 731 SECM	ITIL, ISO 17799, PMBOK, PRINCE2, VAL IT, ISO/IEC 15504-1, ISO/IEC 15504-2	-	ISO 9000, ISO/IEC 2382-1, ISO/IEC 2382-20, ISO/IEC 12207 e ISO/IEC 15288	-
	Tempo de mercado	7 anos	6 anos	2 anos	5 anos	16 anos
Flexibilidade	Rastreabilidade	Sim	Sim	Não	Sim	Não
	Benchmarking	Dependente de método externo	Nativo	Nativo	Nativo	Nativo
	Customização	Sim	Sim	Sim	Sim	Não
Custos (em R$[4])	Custo com capacitação[5]	7.043,40	1.291,29	-	1.080,00	-
	Custo do material[6]	-	469,56	-	555,00	-

[4] Dólar cotado à $2,3478 (taxa média) em 2/12/2013. A taxa se refere à média, ponderada pelo volume, das operações de câmbio da BM&FBOVESPA.
[5]Valores aproximados, referentes aos cursos introdutórios
[6]Valores aproximados, referentes a documentação básica

A partir da estrutura hierárquica de critérios (figura 2) é possível determinar a estrutura de avaliação na técnica AHP, que toma os critérios em pares a fim de submetê-los a uma comparação. Para exemplificar, o critério ‘estrutura’ possui três outros critérios: 'quantidade de níveis', 'descrição das escalas de maturidade' e 'dependência entre níveis'. A comparação é feita da seguinte forma:

O conjunto de critérios apresentados serviram de insumo para a próxima fase do estudo (seleção do modelo), onde um conjunto de cinco especialistas – oriundos dos setores público e privado, com ampla experiência em governança e gestão de riscos – julgou a relevância dos critérios para escolha de um modelo de maturidade no contexto da gestão de riscos de TI.

6. Seleção do Modelo de Maturidade

Para a seleção do modelo de maturidade, foram identificados, inicialmente, um conjunto 23 critérios que, na opinião dos especialistas, deveriam ser considerados para a escolha do modelo. Para obter o consenso confiável de opiniões do grupo de especialistas foi utilizada a técnica Delphi, que permitiu definir com clareza quais critérios o grupo de especialistas tinha consenso sobre sua utilização, sendo assim reduzidos a 13 critérios.

6.1 Estrutura hierárquica de critérios para aplicação da técnica AHP

Para apoiar a escolha do modelo de maturidade, foi utilizada a técnica de decisão multicritério Analytic Hierarchy Process (AHP). Como a técnica exige a definição de uma estrutura hierárquica dos critérios, os treze critérios identificados foram agrupados em cinco categorias (estrutura, concepção, robustez, flexibilidade e custos).

Figura 3: Estrutura hierárquica de critérios utilizados para a avaliação dos modelos de maturidade

A partir da estrutura hierárquica de critérios (figura 2) é possível determinar a estrutura de avaliação na técnica AHP, que toma os critérios em pares a fim de submetê-los a uma comparação. Para exemplificar, o critério ‘estrutura’ possui três outros critérios: 'quantidade de níveis', 'descrição das escalas de maturidade' e 'dependência entre níveis'. A comparação é feita da seguinte forma:

1ª comparação: quantidade de níveis e descrição das escalas de maturidade;

2ª comparação: quantidade de níveis e dependência entre níveis;

3ª comparação: descrição das escalas de maturidade e dependência entre níveis.

Ao todo foram entrevistados seis profissionais, que manifestaram individualmente sua opinião sobre cada um dos critérios (totalizando 69 comparações), que ao final foram combinadas.

6.2 Resultados obtidos a partir da aplicação da técnica AHP

De uma forma geral a técnica AHP deixa claro aos participantes quais objetos estão sendo avaliados. Contudo, nesta pesquisa, foi realizada uma avaliação 'às cegas', pois não foi informado aos entrevistados a relação entre o critério avaliado e o modelo correspondente, de forma a não influenciar a medida de opinião e evitar uma escolha tendenciosa. Os resultados consolidados são exibidos a seguir:

Tabela 2: Pesos obtidos pelos modelos de maturidade estudados

CRITÉRIOS				**C = PESOS N3**				
Critérios N1	**A = Pesos N1**	**Critério N2**	**B = Pesos N2**	**CMMI 1.3**	**COBIT 4.1**	**FVSAH**	**ISO/IEC 15504**	**RMM**
Estrutura	0,204	Quantidade de níveis	0,199	0,358	0,389	0,358	0,389	0,253
		Descrição das escalas de maturidade	0,441	0,413	0,332	0,186	0,332	0,069
		Dependência entre níveis	0,361	0,783	0,783	0,783	0,783	0,217
Concepção	0,347	Domínio do modelo de referência	0,432	0,090	0,278	0,116	0,116	0,517
		Instrumentos de avaliação	0,377	0,144	0,856	0,144	0,144	0,144
		Entidade mantenedora	0,192	0,108	0,334	0,086	0,472	0,086
Robustez	0,177	Alinhamento com outros instrumentos	0,754	0,119	0,626	-	0,255	-
		Tempo de mercado	0,246	0,206	0,269	0,099	0,262	0,165
Flexibilidade	0,204	Rastreabilidade	0,516	0,872	0,872	0,128	0,872	0,128
		Benchmarking	0,207	0,226	0,774	0,774	0,774	0,774
		Customização	0,278	0,653	0,653	0,653	0,653	0,347
Custos	0,068	Custo com capacitação	0,668	0,130	0,363	0,106	0,400	0,106
		Custo do material	0,332	0,485	0,253	0,485	0,262	0,485

A tabela 2 apresenta os valores originais obtidos após a aplicação da técnica AHP e com a consolidação das respostas de todos os entrevistados.

Tabela 3: Pesos ponderados dos critérios avaliados

CRITÉRIOS		D = C x B x A				
Critérios N1	**Critério N2**	**CMMI 1.3**	**COBIT 4.1**	**FVSAH**	**ISO/IEC 15504**	**RMM**
Estrutura	Quantidade de níveis	0,015	0,016	0,015	0,016	0,010
	Descrição das escalas de maturidade	0,037	0,030	0,017	0,030	0,006
	Dependência entre níveis	0,058	0,058	0,058	0,058	0,016
Concepção	Domínio do modelo de referência	0,013	0,042	0,017	0,017	0,078
	Instrumentos de avaliação	0,019	0,112	0,019	0,019	0,019
	Entidade mantenedora	0,007	0,022	0,006	0,031	0,006
Robustez	Alinhamento com outros instrumentos	0,016	0,084	-	0,034	-
	Tempo de mercado	0,009	0,012	0,004	0,011	0,007
Flexibilidade	Rastreabilidade	0,092	0,092	0,013	0,092	0,013
	Benchmarking	0,010	0,033	0,033	0,033	0,033
	Customização	0,037	0,037	0,037	0,037	0,020
Custos	Custo com capacitação	0,006	0,016	0,005	0,018	0,005
	Custo do material	0,011	0,006	0,011	0,006	0,011

Obedecendo à hierarquia definida pelos critérios, os quais também possuem pesos que definem sua relevância em relação aos demais, foram calculados na tabela 3 os pesos ponderados entre os critérios de nível 1, 2 e 3 da tabela 2.

Tabela 4: Resultados finais agrupados pelos critérios de nível 1

CRITÉRIOS	E = RESULTADO FINAL (POR CRITÉRIO DE N1)				
Critérios N1	**CMMI 1.3**	**COBIT 4.1**	**FVSAH**	**ISO/IEC 15504**	**RMM**
Estrutura	0,109	0,103	0,089	0,103	0,032
Concepção	0,040	0,176	0,042	0,068	0,102
Robustez	0,025	0,095	0,004	0,045	0,007
Flexibilidade	0,138	0,162	0,083	0,162	0,066
Custos	0,017	0,022	0,016	0,024	0,016

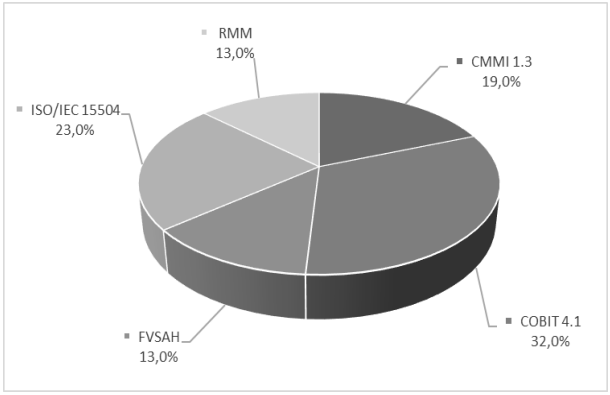
A tabela 4 apresenta os valores da tabela 3 (pesos ponderados pela hierarquia de critérios) agrupados de acordo com os critérios principais (critérios pertencentes ao nível 1). Uma vez calculado o peso ponderado dos critérios, foi possível calcular a pontuação final dos modelos, indicando assim, a preferência dos entrevistados por um determinado modelo.

Tabela 5: Pontuação final obtida pelos modelos de maturidade estudados

PONTUAÇÃO FINAL DOS MODELOS DE MATURIDADE				
CMMI 1.3	**COBIT 4.1**	**FVSAH**	**ISO/IEC 15504**	**RMM**
0,329	**0,558**	**0,234**	**0,402**	**0,223**
19%	32%	13%	23%	13%

De acordo com a tabela 5, é possível verificar a pontuação final obtida por cada modelo, referente à soma dos critérios já ponderados, onde os critérios referentes ao COBIT alcançaram 0,558 pontos, seguido da ISO/IEC 15504 com 0,0402 pontos e CMMI com 0,329 pontos. O modelo FVSAH alcançou 0,234 pontos e o RMM 0,223.

Figura 4: Distribuição dos modelos de maturidade segundo preferência dos entrevistados



Analisando os percentuais obtidos pelos modelos, observa-se que a framework COBIT 4.1 reflete o modelo de maturidade que mais se adequa à preferência dos entrevistados em relação aos critérios apresentados, obtendo 32,0% da pontuação total. O segundo modelo que melhor pontuou foi a ISO/IEC 15504, com 23,0% da preferência, seguido por CMMI 1.3 (18,8%) e tecnicamente empatados os modelos FVSAH (13,4%) e RMM (12,8%).

6.3 Revisão do Modelo de Referência do COBIT

Uma vez definido o modelo de referência (selecionado com base em múltiplos critérios), faz-se necessário o desenvolvimento de um instrumento de avaliação de maturidade em gestão de riscos de TI. Conforme pode ser observado no comparativo, o COBIT sugere um formulário padrão, não automatizado e com baixo nível de detalhamento. O Guia de Auto Avaliação do COBIT 4.1 [23] sugere ao menos dois instrumentos para apoio a auto avaliação. O primeiro instrumento é uma tabela para registro dos resultados da avaliação do processo e o segundo é um modelo para a auto avaliação composto por duas seções. A primeira seção é utilizada para registrar os resultados resumidos da avaliação e a segunda seção é utilizada para registrar de forma detalhada a avaliação. Embora a segunda seção sugira uma avaliação detalhada, sua proposta é ainda genérica, sendo os critérios de avaliação associados aos atributos de processo superficiais e pouco claros. O instrumento de avaliação proposto neste artigo está baseado no modelo de avaliação do COBIT, porém com um nível maior de detalhamento, permitindo uma avaliação mais criteriosa do nível de maturidade do processo de gestão de riscos de TI. O mais recente modelo de maturidade do COBIT deixou de se basear no modelo CMMI e passou a referenciar o modelo proposto na norma ISO/IEC 15504-2. Assim, os seis níveis de maturidade originais foram mantidos, porém com novas descrições e significados. Os níveis de capacidade são apresentados a seguir.

Os níveis de capacidade *incompleto*, *executado* e *gerenciado* tem como foco a visão/conhecimento de uma instância da organização, enquanto que os níveis *estabelecido*, *previsível* e *em otimização* possuem seu foco na organização como um todo. Com base nessas novas considerações, propomos um novo instrumento de avaliação da maturidade do processo de riscos de TI em organizações.

7. Instrumento de avaliação de maturidade em gestão de riscos de TI

O instrumento de avaliação anterior, analisado nesse artigo, apresentava para cada nível de maturidade um conjunto de atributos de processo, que por sua vez continha um outro conjunto de critérios de avaliação. Com o novo instrumento proposto, cada critério de avaliação passa a ter um conjunto de práticas base e produtos de trabalho (definidos com base no Modelo de Referência do Processo PO9 do COBIT 4.1) e associados ao nível 1 e de práticas genéricas e produtos de trabalho genéricos (baseados na norma ISO/IEC 15504) associados aos demais níveis de maturidade.

Assim, o instrumento de avaliação proposto neste artigo adota os 42 critérios de avaliação originais e os desmembra em 112 novos critérios de avaliação, associados aos níveis de maturidade, atributos de processo e critérios de avaliação. A tabela a seguir descreve a distribuição dos novos critérios de avaliação.

O novo instrumento de avaliação desenvolvido, que incorpora novos elementos à avaliação, permitindo à organização avaliada diagnosticar e responder com maior clareza a existência de uma prática ou ainda de um artefato esperado (ou produtos de trabalho), diminuindo assim a chance de respostas subjetivas e aumentando a precisão da avaliação.

Tabela 6: Níveis de capacidade do COBIT 4.1 com base na ISO/IEC 15504- [24]

Níveis de capacidade	**Descrição dos níveis de capacidade (baseado ISO/IEC 15504-2)**	**Contexto**
5 – Em otimização	Continuamente melhorado para atingir os relevantes objetivos atuais e projetados da organização	Visão corporativa / Conhecimento corporativo
4 – Previsível	Opera dentro dos limites definidos para alcançar os resultados dos processos	
3 – Estabelecido	Opera usando um processo definido que é capaz de alcançar seus resultados de processos	
2 – Gerenciado	Implementado de forma gerenciado (planejado, monitorado e ajustado) com produtos de trabalho adequadamente estabelecido, controlado e mantido	Visão da instância / conhecimento individual
1 – Executado	Atinge o propósito do processo	
0 – Incompleto	Não implementado ou pouca/nenhuma evidência para um alcance sistemático do propósito do processo	

Tabela 7: Distribuição dos critérios de avaliação por nível de maturidade, atributo de processo e tipos de evidência

Nível Maturidade	**Atributo de Processo**	**Tipos de Critérios (Evidências)**		**Total**
		Prática	**Produto de Trabalho**	
Nível 1 - Executado	PA 1.1 Execução do processo	9	14	**23**
Nível 2 - Gerenciado	PA 2.1 Gerência de execução	6	10	**16**
	PA 2.2 Gerência de produto de trabalho	4	5	**9**
Nível 3 - Estabelecido	PA 3.1 Definição de processo	5	6	**11**
	PA 3.2 Implementação de processo	6	7	**13**
Nível 4 - Previsível	PA 4.1 Medição de processo	6	7	**13**
	PA 4.2 Controle de processo	5	6	**11**
Nível 5 - Em otimização	PA 5.1 Inovação de processo	5	5	**10**
	PA 5.2 Otimização de processo	3	3	**6**
Totais		**49**	**63**	**112**

Conforme pode ser visto na tabela 8, os 112 critérios de avaliação são distribuídos pelos nove atributos de processo que determinam os níveis de maturidade. Cada atributo de processo possui um conjunto de critérios de avaliação, que agora são agrupados em práticas (49) e produtos de trabalho (63), que ajudam a evidenciar o seu alcance. O instrumento desenvolvido permite o registro dos dados coletados junto à organização avaliada ao mesmo passo que automatiza o processo de avaliação. A avaliação é feita com base nas respostas registradas no formulário acima, onde cada questão deve ser respondida com 'S' (sim) ou 'N' (não), de forma a indicar se a prática ou o produto de trabalho esperado se encontra completamente implementado ou não.

Após o preenchimento do questionário deve ser calculado o índice de capacidade de cada um dos atributos de processo (1). Para isso, é utilizada a seguinte fórmula:

$$ICAP = \frac{QRA}{TQA} * 100 \quad (1)$$

Sendo:

ICAP = Índice de Capacidade do Atributo de Processo

QRA = Quantidade de Respostas Afirmativas

TQA = Total de Questões Avaliadas

Após calcular os índices para cada um dos processos é necessário determinar os níveis de capacidade alcançados. Para isso é utilizada uma escala ordinal composta pelos seguintes valores:

Tabela 8: Nível de capacidade dos atributos de processo [24] [23]

Valor	Significado	Escala de avaliação
N	Não atingido	0 a 15% de alcance
P	Parcialmente atingido	> 15% a 50% de alcance
L	Amplamente atingido	> 50% a 85% de alcance
F	Completamente atingido	> 85% a 100% de alcance

A classificação N (não atingido) é utilizada quando não há evidencias do alcance do atributo definido no processo em análise. A classificação P (parcialmente atingida) é utilizada quando existe alguma evidencia de alcance do atributo, sabendo que alguns aspectos do atributo podem ser imprevisíveis. Já a classificação L (amplamente atingido) é utilizada quando existe evidência de alcance sistemático e significativo do atributo, sabendo que podem existir alguns pontos fracos relacionados a ele. Por fim, a classificação F (completamente atingido) é utilizada quando existe uma adesão completa e sistemática e de alcance total do atributo avaliado.

Para a definição do nível de maturidade do processo, deve ser analisado individualmente o nível de capacidade dos atributos de processo. De uma forma geral, para alcançar um nível de capacidade, o atributo de processo analisado deve obter uma classificação L (amplamente atingido) ou F (completamente atingido) e seus atributos de processo dos níveis inferiores devem obter uma classificação F (completamente atingido).

Tabela 9: Requisitos para pontuação em um nível de capacidade [23]

Escala	Atributos de processo	Pontuação
Nível 1	Execução do processo	Amplamente ou completamente
Nível 2	Execução do processo	Completamente
	Gerência de execução	Amplamente ou completamente
	Gerência de produto de trabalho	Amplamente ou completamente
Nível 3	Execução do processo	Completamente
	Gerência de execução	Completamente
	Gerência de produto de trabalho	Completamente
	Definição de processo	Amplamente ou completamente
	Implementação de processo	Amplamente ou completamente
Nível 4	Execução do processo	Completamente
	Gerência de execução	Completamente
	Gerência de produto de trabalho	Completamente
	Definição de processo	Completamente
	Implementação de processo	Completamente
	Medição de processo	Amplamente ou completamente
	Controle de processo	Amplamente ou completamente
Nível 5	Execução do processo	Completamente
	Gerência de execução	Completamente
	Gerência de produto de trabalho	Completamente
	Definição de processo	Completamente
	Implementação de processo	Completamente
	Medição de processo	Completamente
	Controle de processo	Completamente
	Inovação de processo	Amplamente ou completamente
	Otimização de processo	Amplamente ou completamente

O nível 0 (incompleto) não considera nenhum atributo de processo. A partir do nível 1 são avaliados os atributos de processo como requisitos para um determinado nível de capacidade, que leva em consideração não só os atributos de processo que são requisitos para aquele nível, mas também atributos de processo do nível anterior.

8. Considerações finais

Neste estudo foi possível observar a existência de diversos modelos de maturidade com características e finalidades distintas. O estudo comparativo aqui apresentado, produziu como resultado uma matriz comparativa que descreve de forma sistemática e objetiva as principais características dos modelos de maturidade a partir das perspectivas de estrutura, concepção, robustez, flexibilidade e custos.

Embora qualquer um dos modelos estudados possa ser utilizado em um processo de avaliação de maturidade, o COBIT foi o modelo que apresentou uma maior aderência aos critérios definidos pelos especialistas, que com base na técnica de decisão multicritério AHP (Analytic Hierarchy Process) obteve a maior pontuação e se mostrou mais adequado ao a avaliação de maturidade da gestão de riscos de TI.

O novo método para aplicação da técnica AHP, onde os objetos comparados não foram explicitamente declarados, mas substituídos por suas características, permitiu uma avaliação mais imparcial, diminuindo a chance de influência sobre a escolha por preferências pessoais. A aplicação da técnica permitiu a tomada de decisão a partir da opinião de todos os envolvidos e a quantificação dos critérios permitiu demonstrar o grau de preferência de um determinado critério em detrimento a outros.

Um instrumento para avaliação de maturidade em gestão de riscos de TI foi definido com base no modelo de avaliação de processo do COBIT 4.1. Neste instrumento os 42 critérios originais foram expandidos para 112 novos critérios, permitindo assim uma avaliação mais detalhada, com respostas menos subjetivas e com maior precisão na avaliação dos atributos de processo, porém mantendo o alinhamento com os critérios originais.

Espera-se este artigo induza o desenvolvimento de trabalhos futuros para ampliação da pesquisa e desenvolvimento de novos artefatos. A pesquisa para escolha do modelo de maturidade, por exemplo, poderá ser ampliada a partir da inclusão de novos critérios. Outra aplicação possível é o uso da solução apresentada para avaliação de maturidade em outras organizações que desenvolvam atividades de gestão de riscos em TI, de forma a permitir não somente a identificação do seu nível de maturidade, mas também o benchmarking entre elas.

Por fim, acredita-se que a avalição de maturidade do processo de gestão de riscos de TI permite a uma organização, além de identificar o seu nível atual de maturidade, conhecer os caminhos para evolução de seus processos de governança de TI, através do monitoramento e análise crítica em busca da melhoria contínua de seu processo de gestão de riscos.

Referências

[1] ITGI – IT Governance Institute. COBIT 4.1. Illinois - USA, 2007. Disponível em: <http://www.isaca.org/Knowledge-Center/cobit/Pages/Downloads.aspx>. Acesso em: 30 jun. 2017.

[2] IBGC – Instituto Brasileiro de Governança Corporativa. Código das melhores práticas da governança corporativa. 5ª edição, São Paulo, 2009. Disponível em: <http://www.ibgc.org.br/userfiles/2014/files/CMPGPT.pdf>. Acesso em: 30 jun. 2017.

[3] WEILL, P.; ROSS, J. W. Governança de TI. *Tecnologia da Informação*. São Paulo: M. Books, 2006.

[4] ISO – International Organization for Standardization. ISO/IEC 15504-1:2004 Information technology – Process assessment. *Part 1: Concepts and vocabulary*. 2004.

[5] HOPKINSON , M. Improving Risk Management Capability Using the Project Risk Maturity Model. *A Case Study Based on UK Defence Procurement Projects*. PM World Today. vol. XIII. October, 2011.

[6] SHAHZAD, B.; SAFVI, S. A. Risk mitigation and management scheme based on risk priority. Global Journal of Computer Science and Technology, vol. 10, nº Issue 4, pp. 108-113, 2010.

[7] HOLANDA, A. B. d. I.. Novo Dicionário Eletrônico Aurélio. Positivo, 2004.

[8] ISO - International Organization for Standardization. ISO Guide 73:2009 Risk Management. *Vocabulary*.

2009.

[9] HM TREASURY - Her majesty's Treasury. The Orange Book. p. 52. Norwich: Crown, 2004.

[10] ELMAALLAM, M. K. A. Towards a model of maturity for is risk management. *International Journal of Computer Science & Information Technology*. vol. 3, nº 4. August, 2011.

[11] RAMOS, A. et al. Security Officer. *Guia Oficial para Formação de Gestores de Segurança da Informação*. 2ª ed., vol. I, Porto Alegre: Zouk, 2008.

[12] SILVEIRA, A. D. M. d., Governança Corporativa no Brasil e no Mundo. *Teoria e Prática*, Rio de Janeiro: Elsevier, 2010.

[13] SEI Software Engineering Institute. CMMI for Services. Carnegie Mellon, Pittsburgh, 2010.

[14] DSIC – Departamento de Segurança da Informação e Comunicações. Norma Complementar nº 04/IN01/DSIC/GSIPR – Diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações. Disponível em: <http://dsic.planalto.gov.br/documentos/nc_04_grsic.pdf>. Acesso em: 30 jun. 2017.

[15] COSO – Committee of Sponsoring Organizations of the Treadway Commission. Gerenciamento de Riscos Corporativos – Estrutura Integrada. *Sumário Executivo e Estrutura*. 2007

[16] ISO – International Organization for Standardization. ISO 31000:2009 Risk management. *Principles and guidelines*. 2009.

[17] OECD – Organization for Economic Co-operation and Development. Principles of Corporate Governance. 2004. Disponível em:

<http://www.oecd.org/corporate/corporateaffairs/corporategovernanceprinciples/31557724.pdf>. Acesso em: 30 jun. 2017.

[18] ISO – International Organization for Standardization. ISO/IEC38500:2008 Corporate governance of information technology. 2008.

[19] SAATY, T. L. Extending the Measurement of Tangibles to Intangibles. International Journal of Information Technology & Decision Making, vol. 8, pp. 7-27, 2009.

[20] VARGAS, R. V. The History of Risk Management. *Based on the book Against The God*. 2009. Disponível em: <http://www.ricardo-vargas.com/slides/20>. Acesso em: 30 jun. 2017.

[21] SILVA, J. M. d. Apostila de Formação de valor em sistemas de atividades humanas. Faculdade de Tecnologia, Núcleo de Engenharia de Produção, UnB, 2012.

[22] HILLSON, D. A. Towards a Risk Maturity Model. The International Journal of Project & Business Risk Management., vol. I, nº I, pp. 35-45, Spring 1997.

[23] ISACA – Information Systems Audit and Control Association. COBIT Self-assessment Guide: *Using COBIT 4.1*. Illinois - USA, 2011.

[24] ISACA – Information Systems Audit and Control Association. COBIT Process Assessment Model (PAM): *using COBIT 4.1*. Illinois - USA, 2011.

[25] SEI – Software Engineering Institute, Standard CMMI Appraisal Method for Process Improvement (SCAMPI) A Version 1.3: *Method Definition Document.* Carnegie Mellon, Pittsburgh, PA, March, 2011.