Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Ciência da Computação

Análise de Maturidade da Gestão de Riscos de TI na Fiocruz: definição e aplicação de instrumento de avaliação e especificação de requisitos para um sistema computacional

Misael Sousa de Araújo

Dissertação apresentada como requisito para conclusão do
Mestrado Profissional em Computação Aplicada

Orientador

Prof. Dr. Edgard Costa Oliveira

Brasília

2014

Universidade de Brasília – UnB

Instituto de Ciências Exatas

Departamento de Ciência da Computação

Computação Aplicada

Coordenador: Prof. Dr. Marcelo Ladeira

Banca examinadora composta por:

Prof. Dr. Edgard Costa Oliveira (Orientador) – ENE/FT/UnB

Prof. Dr. Marcello Sandi Pinheiro – CDS/EB

Prof.ª Dr.ª Simone Borges Simão Monteiro – EPR/FT/UnB

CIP – Catalogação Internacional na Publicação

Ficha catalográfica elaborada pela Biblioteca Central da Universidade de Brasília. Acervo 1015895.

A663a

Araujo, Misael Sousa de.
Análise de maturidade da gestão de riscos de TI na Fiocruz : definição e aplicação de instrumento de avaliação e especificação de requisitos para um sistema computacional / Misael Sousa de Araujo. -- 2014.
174 f. : il. ; 30 cm.

Dissertação (mestrado) - Universidade de Brasília, Departamento de Ciência da Computação, Programa de Mestrado Profissional em Computação Aplicada, 2014.
Inclui bibliografia.
Orientação: Edgard Costa Oliveira.

1. Fundação Oswaldo Cruz. 2. Administração de risco. 3. Modelos de capacitação e maturidade (Software). 4. Tecnologia da informação. 5. COBIT (Modelo de gestão de Tecnologia da Informação). I. Oliveira, Edgard Costa. II. Título.

CDU 658:004

Endereço: Universidade de Brasília

Campus Universitário Darcy Ribeiro – Asa Norte

CEP 70910-900

Brasília – DF – Brasil

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Ciência da Computação

Análise de Maturidade da Gestão de Riscos de TI na Fiocruz: definição e aplicação de instrumento de avaliação e especificação de requisitos para um sistema computacional

Misael Sousa de Araújo

Dissertação apresentada como requisito para conclusão do
Mestrado Profissional em Computação Aplicada

Prof. Dr. Edgard Costa Oliveira (Orientador)
FGA/UnB

Prof.ª Dr.ª Simone Borges Monteiro Simão
EPR/UnB

Prof. Dr. Marcello Sandi Pinheiro
Exército Brasileiro - CDS

Prof. Dr. Marcelo Ladeira
Coordenador do Programa de Pós-graduação em Computação Aplicada

Brasília, 15 de maio de 2014

Dedicatória

Aos meus pais pelo amor e dedicação de suas vidas a mim e a minha querida esposa Grace Kelly pelo estímulo e carinho, dedico-lhes essa conquista com gratidão.

Agradecimentos

Agradeço primeiramente a Deus, autor da minha fé, a quem devo a vida, o que tenho e o que sou. Agradeço ainda aos meus pais, Nilton e Severina, pela educação e dedicação de longos anos. À minha esposa Grace Kelly pela paciência, apoio e compreensão durante o curso. Aos meus irmãos Daniel e Luciano, grandes incentivadores e apoiadores. Ao Dr. Pedro Ribeiro Barbosa, Vice-Presidente da Fiocruz, por acreditar e incentivar este projeto. Ao coordenador de TI da Fiocruz, Álvaro Funcia Lemme, pelos inúmeros conselhos e palavras de encorajamento. Aos amigos Flávio Luiz, Ricardo Moraes e Rubens Ferreira que me apoiaram de diversas maneiras durante todo o curso. Agradeço ainda a todos os colegas da linha de pesquisa de Gestão de Riscos que acolheram o 'forasteiro carioca', em especial Artur Winter e Antonio Marcos. Deixo ainda um último e especial agradecimento ao meu orientador e amigo, Dr. Edgard Costa Oliveira, pela confiança, paciência, dedicação, serenidade e inteligência com que me trouxe até o fim desta jornada.

"O que vale na vida não é o ponto de partida e sim a caminhada.
Caminhando e semeando, no fim terás o que colher"

Cora Coralina

Resumo

A gestão de riscos constitui uma importante área de conhecimento para o processo de governança, permitindo que riscos sejam conhecidos e adequadamente tratados, fornecendo informações precisas para a tomada de decisão a partir de atividades coordenadas que dirigem uma organização. Um fator relevante para o sucesso da gestão de riscos é conhecer o quanto uma organização implementa de forma consistente o seu processo de gestão de riscos, pois sua eficiência contribuirá para o atendimento dos objetivos de negócio da instituição. No entanto, quais são as características dos principais modelos de maturidade disponíveis para aplicação no contexto da gestão de riscos de TI? Qual modelo de maturidade adotar como referência? Quais critérios utilizar para escolha do modelo? Que instrumentos utilizar para a avaliação de maturidade? Buscou-se responder a essas questões por meio dos objetivos propostos nesta pesquisa, que apresenta uma análise comparativa de modelos de maturidade, define critérios e método para a escolha de um modelo de maturidade alinhado à expectativa da organização, define um instrumento de avaliação, especifica os requisitos para construção de um sistema computacional para coleta de dados sobre o processo de gestão de riscos de TI e avaliação do seu nível de maturidade, e valida o instrumento e requisitos através da sua aplicação na instituição. Foram utilizadas diversas técnicas para coleta de dados: entrevistas, questionários, formulários, pesquisas documentais e bibliográficas, além da técnica de decisão multicritério *Analytic Hierarchy Process* (AHP). Foi possível observar que existem vários modelos de maturidade, com finalidades e características distintas, presentes em *frameworks* como CMMI, COBIT, ERM, FVSAH, ISO 15504 e RMM, onde o modelo de maturidade mais adequado para o escopo proposto foi o do COBIT 4.1. A técnica AHP se mostrou adequada como método para escolha do modelo de maturidade. A solução proposta é composta por um instrumento de avaliação, a especificação de requisitos para um sistema computacional para coleta de dados e avaliação de maturidade e *templates* de produtos de trabalho para a documentação do processo. Espera-se que este estudo estimule trabalhos futuros, como a ampliação da pesquisa e aplicação em outras organizações dos instrumentos desenvolvidos, promovendo a melhoria dos processos de gestão de riscos e governança de TI.

Palavras-Chave: Gestão de Riscos, Análise de Maturidade em TI, Governança de TI, COBIT, Fiocruz.

Abstract

Risk management is an important area of knowledge to the process of governance, allowing risks be known and treated appropriately, providing accurate information for decision making from coordinated activities that drive an organization. A relevant factor for the success of risk management is knowing how much an organization implements consistently its process of risk management, because its efficiency will contribute to meeting the business goals of the institution. However, what are the main characteristics of the maturity models available for application in the context of risk management of IT? Which maturity model to adopt as a reference? Which criteria to use to select the model? What instruments used for assessment of maturity? We attempted to answer these questions through the proposed objectives in this research, that presents a comparative analysis of maturity models, define criteria and method for selecting a maturity model aligned to the expectations of the organization, defines an evaluation instrument, specifies the requirements for building a computational system for collecting data on the process of managing risks IT and assessment of their level of maturity, and validates the instrument and requirements through its application in the institution. Several techniques for data collection were used: interviews, questionnaires, forms, both bibliographic and documentary research, beyond the technique of multicriteria decision Analytic Hierarchy Process (AHP). Was observed that there are many maturity models with distinct characteristics and purposes, present in frameworks like CMMI, COBIT, ERM, FVSAH, ISO 15504 and RMM, where the most appropriate maturity model for the scope proposed was the COBIT 4.1. The AHP technique proved suitable as a method for choosing the maturity model. The proposed solution consists of an assessment tool (developed in Excel), the specification of requirements for a computer system for data collection and evaluation of maturity and work products templates for the process documentation. It is hoped that this study stimulate further work, such as the expansion of research and application of the tools developed in other organizations, promoting the improvement of the processes of risk management and IT governance.

Keywords: Risk Management, IT Maturity Assessment, IT Governance, COBIT, Fiocruz.

Lista de Figuras

Lista de Tabelas

Lista de Abreviaturas e Siglas

ABNT	Associação Brasileira de Normas Técnicas
AHP	*Analytic Hierarchy Process*
CETIC	Centro de Estudos sobre as Tecnologias de Informação e da Comunicação
CGTI	Coordenação de Gestão de Tecnologia da Informação
CMMI	*Capability Maturity Model Integration*
COBIT	*Control Objectives for Information and Related Technology*
COSO	*Committee of Sponsoring Organization of the Treadway Commission*
CTIR.Gov	Centro de Tratamento de Incidentes de Segurança de Redes
DSIC	Departamento de Segurança da Informação e Comunicações
EGTI	Estratégia Geral de Tecnologia da Informação
ERM	*Entreprise Risk Management*
FIOCRUZ	Fundação Oswaldo Cruz
FVSAH	Formação de Valor em Sistemas de Atividades Humanas
GSI	Gabinete de Segurança Institucional
IIA	*Institute of Internal Auditors*
IBGC	Instituto Brasileiro de Governança Corporativa
IEC	*International Eletrotechnical Comission*
ISACA	*Information Systems Audit and Control Association*
ISO	*International Organization for Standardization*
ITGI	*IT Governance Institute*
OECD	*Organization for Economic Co-operation and Development*
PWC	*PricewaterhouseCoopers*
RMM	*Risk Maturity Model*
RMMM	*Risk Management Maturity Model*
SEFTI	Secretaria de Fiscalização de Tecnologia da Informação
SEI	*Software Engineering Institute*
SISP	Sistema de Administração dos Recursos de Tecnologia da Informação
SUS	Sistema Único de Saúde
TCU	Tribunal de Contas da União

Sumário

Capítulo 1

Introdução

1.1. Contextualização

A informação é hoje um dos principais recursos das organizações, sendo a todo instante criada, utilizada, armazenada, divulgada, compartilhada e destruída (IIA, 2004). As tecnologias de informação têm estado mais presentes no dia a dia das organizações e são consideradas fator crítico para o seu sucesso ou fracasso. Observa-se um aumento expressivo do uso e dependência das tecnologias de informação, onde contribuiu para este cenário o crescimento da Internet na última década (CETIC, 2011) e sua consolidação como canal predominante na obtenção de serviços públicos (CETIC, 2010).

Outro fator que corroborou para o aumento dos serviços e informações disponibilizadas ao cidadão foi a publicação da Lei 12.527/11, que assegura o direito fundamental de acesso à informação e fortalece a prestação de serviços públicos (BRASIL, 2011), provocando um aumento da interação entre cidadãos, empresas e órgãos de governo. Para o *IT Governance Institute – ITGI* "as organizações devem satisfazer os requisitos de qualidade, guarda e segurança de suas informações e garantir que a área de TI suporte os objetivos de negócios da organização" (ITGI, 2007).

Com a dependência cada vez maior dos serviços de TI, cresce a expectativa das organizações sobre uma área de TI eficiente e capaz de suportar adequadamente seus objetivos. Segundo o *Information Systems Audit and Control Association – ISACA*, espera-se que a TI gere valor para a organização através da manutenção da qualidade da informação, da promoção do uso eficaz e inovador das informações para o alcance dos objetivos estratégicos, da otimização do custo dos serviços de TI e do alcance da excelência operacional através da aplicação confiável e eficiente da tecnologia (ISACA, 2012a).

O cenário descrito acima não é diferente ao olharmos para o serviço público. Diante desse contexto, as áreas de TI das instituições públicas têm se preocupado em buscar o fortalecimento de seus processos de governança. Esse fato se deve basicamente a dois fatores: maior orientação e regulação do governo (através de publicações como estratégias, instruções normativas, normas complementares, guias, acórdãos, etc.) e uma cobrança da sociedade por serviços públicos de qualidade, principalmente após a publicação da Lei de Acesso à Informação, que mudou radicalmente o modo como as organizações prestam contas à sociedade.

Tendo em vista a relevância da TI para as organizações, a governança em TI se constitui em um grande desafio, especialmente devido a sua estreita relação com o processo de governança corporativa, não podendo ser dela desassociada. Hoje, é possível entender a governança de TI como parte do processo de governança corporativa e a gestão de riscos como um instrumento de extrema importância para quaisquer processos da organização. Segundo o *IT Governance Institute – ITGI, "o*rganizações bem-sucedidas entendem e gerenciam os riscos em seus processos de governança de TI" (ITGI, 2007, p. 8).

Se por um lado o uso intensivo das tecnologias de informação traz mais competitividade e transparência à organização, por outro, traz novos riscos e desafios. Embora tenha se tornado o principal canal para obtenção de serviços e um componente importante no processo de governança, a área de TI desperta preocupação em seus dirigentes quanto aos riscos a que estão expostos.

Uma pesquisa da empresa *PricewaterhouseCoopers – PwC*, sobre 'o que mais preocupa líderes brasileiros', para 71% dos entrevistados a maior preocupação é com ataque cibernético ou um colapso na Internet. Essa preocupação se justifica pela relevância da TI enquanto área chave que suporta os principais processos de negócio das organizações, sejam elas públicas ou privadas (PWC, 2013b).

Outra pesquisa, desta vez realizada pela empresa *Trend Micro – TM*, sobre os 'desafios de segurança cibernética enfrentados por economias em rápido crescimento', revela que, na América Latina, 38% dos e-mails maliciosos enviados e 58% das URL's maliciosas hospedadas, tem sua origem no Brasil, colocando o país em primeiro lugar no *ranking* de hosts explorados para práticas maliciosas (TM, 2013).

Ao analisarmos o cenário do governo, as ameaças aos recursos de TI se mostram igualmente preocupantes. Somente nos três primeiros meses de 2013, segundo estatísticas de incidentes de redes divulgadas pelo Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública

Federal – CTIR.Gov, foram confirmados mais de 2000 incidentes de segurança da informação (CTIR, 2013, p. 1).

Um dos instrumentos relevantes para o processo de governança é a gestão de riscos. Segundo o Gabinete de Segurança Institucional da Presidência da República – GSI (GSI, 2008, p. 2), a gestão de riscos é considerada uma atividade integrada da gestão da segurança da informação. Ramos também afirma que a gestão de riscos é "provavelmente um dos componentes mais importantes da Gestão da Segurança da Informação como um todo" (RAMOS, 2008). Para a PwC (2007a), o gerenciamento de riscos possibilita aos gestores tratar com eficácia as incertezas, bem como os riscos e as oportunidades a elas associadas, a fim de melhorar a capacidade de gerar valor.

Assim, as organizações têm adotado a gestão de riscos como um instrumento que as ajude a alcançar seus objetivos de negócio. O *Software Engineering Institute – SEI* (2010) destaca que o quanto antes os riscos forem identificados e tratados, mais fácil, menos dispendioso e menos prejudicial será o processo de gestão de riscos ao se realizar mudanças e correções. Segundo Weill & Ross (2006) um processo de governança de TI mal concebida pode "acarretar frustações tais como gastos desnecessários, aumento de despesas operacionais, interrupção das operações e iniciativas que sustentam, mas não melhoram o desempenho".

A necessidade da avaliação do valor de TI, o gerenciamento dos riscos e as crescentes necessidades de controle sobre as informações são agora entendidos como elementos-chave da governança (ITGI, 2007). Além de prevenir, detectar e corrigir eventos indesejáveis, a gestão de riscos visa prover à direção da organização informações disponíveis e corretas para a tomada de decisões.

É sabido que a adoção de um processo de gestão de riscos contribui para o processo de governança. Controles efetivos reduzem riscos, aumentam a probabilidade da entrega de valor e aprimoram a eficiência, pois existirão poucos erros e o enfoque de gerenciamento será mais consistente (ITGI, 2007, p. 16). Vale ressaltar que o processo para uma transformação significativa da capacidade de gestão de riscos na organização é demorado, demandando esforço e tempo (HOPKINSON, 2011a).

"Tomar decisões levando em consideração os componentes dos riscos é a melhor forma de buscar objetivos para as nossas ações e garantir que elas se encontram dentro de patamares razoáveis" (RAMOS, 2008, p. 84). No entanto, para o aperfeiçoamento do processo de gestão de riscos na organização, faz-se

necessário avaliar continuamente seu nível de maturidade, de forma a identificar suas deficiências e traçar planos de ação que permitam promover sua melhoria.

No mercado atual, existem modelos de maturidade, padrões, metodologias e diretrizes que podem auxiliar uma organização a melhorar sua forma de fazer negócios (SEI, 2010). Segundo pesquisa realizada pelo *Software Engineering Institute* (2010), as organizações se concentram em três dimensões críticas: pessoas, procedimentos e métodos, e ferramentas e equipamentos. Os processos de negócio da organização são utilizados para manter a coesão entre esses três elementos, não significando que as pessoas e a tecnologia não sejam importantes. Porém, o foco em processo permite obter os fundamentos necessários para enfrentar suas constantes mudanças e maximizar a produtividade das pessoas e o uso da tecnologia.

Segundo a ABNT (2008a), a adoção de um *framework* na avaliação de um processo facilita a sua auto avaliação, gera uma pontuação do processo, trata a habilidade do processo para atingir seu propósito, é apropriado a todos os domínios de aplicação e organizações de qualquer tamanho, além de poder prover uma comparação objetiva das organizações.

O Governo Federal tem estimulado a adoção da gestão de riscos como forma das organizações aumentarem sua capacidade de lidar com riscos em seus planos estratégicos, programas, projetos e processos finalísticos. O Programa Nacional de Gestão Pública e Desburocratização – GesPública tem por finalidade melhorar a qualidade dos serviços públicos prestados aos cidadãos e aumentar a competividade do país. Dentre as várias ações do GesPública (carta de serviços, gestão de processos, pesquisa de opinião padronizada, indicadores de desempenho, entre outros), destaca-se o desenvolvimento de um guia para o gerenciamento de riscos, como um instrumento para o contínuo desenvolvimento da gestão e capacidade de governança das organizações (MPOG, 2013).

O Sistema de Administração dos Recursos de Tecnologia da Informação – SISP também incentiva a adoção de práticas de gerenciamento de riscos como uma iniciativa estratégica, conforme pode ser observado na Estratégia Geral de Tecnologia da Informação - EGTI (SISP, 2013, p. 24). O Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República foi além, e estabeleceu diretrizes para o processo de Gestão de Riscos com foco em segurança da informação, com aplicação nos órgãos ou entidades da Administração Pública Federal, direta e indireta (DSIC, 2009).

Diante deste cenário, podemos perceber que, no setor público a TI tem assumido um papel importante na interação entre cidadãos, empresas e governo, sendo área chave na prestação de serviços. A adoção de um processo de gestão de

riscos assume uma posição de destaque nas organizações e a avaliação do seu nível de maturidade se faz necessário não só para compreensão da sua situação atual, mas também para seu contínuo aperfeiçoamento.

1.2. A Fundação Oswaldo Cruz

A Fundação Oswaldo Cruz - Fiocruz é uma organização de Ciência e Tecnologia em Saúde, responsável pela realização de pesquisa, desenvolvimento tecnológico e educação no campo da saúde, além da produção de insumos estratégicos para o Sistema Único de Saúde - SUS. As atividades realizadas pela Fiocruz compreendem especialmente a pesquisa biomédica e a formação em ciência e tecnologia em saúde; a pesquisa clínica e atenção de referência em doenças infecciosas e na área da saúde da mulher, criança e adolescente; a pesquisa epidemiológica e social; a pós-graduação em saúde pública e a formação de nível técnico em saúde; a produção de imunobiológicos, reagentes e medicamentos; a preservação do patrimônio histórico cultural da saúde e a difusão científica e tecnológica.

Desde que foi fundada em 25 de maio de 1900, a Fiocruz tem colocado seu conhecimento a serviço da população brasileira, buscando, através da inovação tecnológica e social, melhorar as condições de vida e saúde de todos. A Fiocruz está presente em dez estados brasileiros e conta com cerca de 12.800 colaboradores. O campus principal, no Rio de Janeiro, possui mais de 800.000m^2. Ao todo, são dezesseis unidades técnico-científicas (voltadas para ensino, pesquisa, inovação, assistência, desenvolvimento tecnológico e extensão no âmbito da saúde), uma unidade técnica de apoio (produção de animais de laboratório e derivados de animais) e quatro unidades técnico-administrativas (dedicadas ao gerenciamento físico da Fundação, às suas operações comerciais e à gestão econômico-financeira).

Em 2010 foi constituída a Coordenação de Gestão de Tecnologia da Informação – CGTI, que passou a responder pela operacionalização dos serviços de TI em quatro unidades técnico-administrativas e Presidência da Fiocruz. Além do seu papel operacional nessas unidades, a CGTI assumiu a responsabilidade de coordenar os projetos estruturantes da instituição, bem como a promoção de políticas e diretrizes institucionais de TI.

A CGTI é constituída por cinco serviços apresentados no diagrama abaixo:

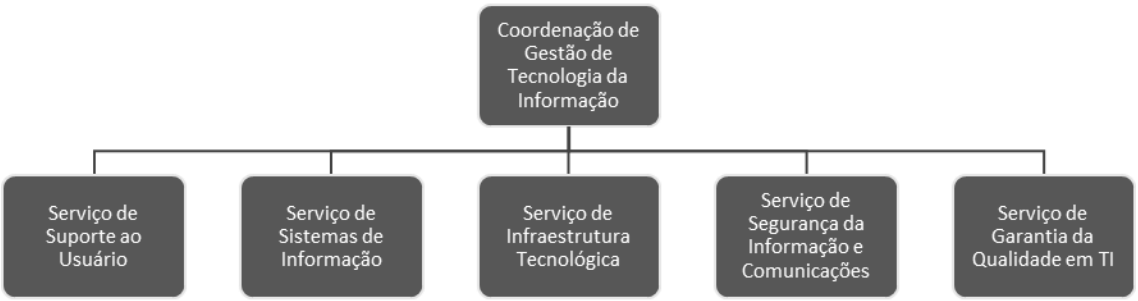


Figura 1: Organograma da Coordenação de Gestão de TI.

A área de suporte é a responsável direta pelo atendimento de 1.500 usuários, distribuídos em 5 unidades e 10 localidades, com um volume médio mensal de 1.400 atendimentos. A área de infraestrutura tecnológica tem a responsabilidade de gerir os 50 km de fibra ótica e mais de 200 ativos críticos (servidores, equipamentos de conectividade, etc.). A área de garantia da qualidade conduz o Planejamento de TI das 16 áreas de TI da instituição, cujo orçamento é da ordem de R$ 65 milhões, sendo R$ 18 milhões em projetos da própria CGTI. Sua área de sistemas é responsável por mais de 100 aplicações das mais diversas áreas e finalidades. A área de segurança da informação é responsável por conduzir a proposição de políticas institucionais sobre o tema através do Comitê de Segurança da Informação, bem como gerir os incidentes de segurança, os planos de continuidade e os riscos inerentes à área de tecnologia da informação. Ao todo são 75 profissionais atuando em regime 24 x 7 para a manutenção dos serviços de TI em níveis aceitáveis (a partir de critérios internos de aceitação de riscos).

Dada a diversidade das atividades realizadas na instituição, sua distribuição geográfica, a quantidade de trabalhadores e a relevância da TI para a prestação de serviços, a governança de TI se revela um grande desafio. Assim, esta pesquisa visa reduzir incertezas quanto ao nível de maturidade da CGTI na gestão de riscos de TI, bem como contribuir para o objetivo estratégico constante no plano quadrienal da instituição de "inovar o modelo de gestão através da adoção da gestão de riscos" (Fiocruz, 2011).

O tema 'gestão de riscos' tem sido um ponto de atenção constante da alta direção da Fiocruz. No Relatório de auto avaliação Fiocruz – Ciclo 2013 para o programa GesPública é colocada a seguinte questão:

> Como são identificados, classificados, analisados e tratados os riscos organizacionais mais significativos que possam afetar a governabilidade e a capacidade da organização de alcançar os seus objetivos estratégicos e de realizar sua missão? (FIOCRUZ, 2013).

A pergunta acima pode ser entendida como uma preocupação da organização com sua capacidade na realização de atividades relativas à gestão de riscos e como isso impacta a organização no alcance de seus objetivos.

O mesmo relatório elenca os principais riscos assumidos pela alta direção, dentre os quais apresenta um risco específico para a área de tecnologia da informação, conforme pode ser observado no item VI, do critério 1.1.C, que diz: "Risco relacionado à gestão da informação na instituição, impactado diretamente sobre a coordenação das ações de Tecnologia da Informação" (FIOCRUZ, 2013).

Até o ano de 2010 cada unidade da Fiocruz possuía uma área de tecnologia da informação, não existindo até então uma área central que respondesse pelas questões de TI de forma institucional. A partir da constituição da Coordenação de Gestão de Tecnologia da Informação – CGTI, a Fiocruz passou a contar com um órgão seccional atuante junto ao Sistema de Administração dos Recursos de Tecnologia da Informação – SISP do Governo Federal sobre as questões de governança de tecnologia da informação, sendo a instância responsável pela articulação das políticas institucionais junto às áreas de TI das unidades, denominada unidades de TI correlatas. Assim, as atividades de gestão de riscos de TI na Fiocruz impõem alguns desafios:

a) Definir um modelo de gestão de riscos de TI em nível institucional;
b) Promover articulação das atividades de gestão de riscos em TI desenvolvidas pela CGTI e unidades de TI correlatas;
c) Padronizar os diferentes critérios para avaliação dos riscos;
d) Padronizar as diferentes ferramentas e técnicas, que produzem:
    i. Resultados em diversas formas de apresentação;
    ii. Resultados não integrados;
    iii. Desconhecimentos dos riscos de forma consolidada;
    iv. Custos elevados;
e) Conhecer o nível de maturidade em gestão de riscos de TI na organização;

A partir de 2012 se observa um aumento no número de incidentes de segurança da informação na instituição. Esses incidentes trazem riscos significativos não somente à segurança das informações e ao processo de governança de TI, mas também afetam todo o processo de governança corporativa, reforçando assim a necessidade de adoção de uma estratégia proativa de identificação e prevenção desses eventos em nível institucional.

Nos últimos anos, os órgãos de controle do governo, em especial o Tribunal de Contas da União - TCU – através da Secretaria de Fiscalização de Tecnologia

da Informação - SEFTI – tem acompanhado a situação da governança de TI nos órgãos da Administração Pública Federal. Em um panorama traçado em 2007, o Tribunal de Contas da União – TCU, através do Acórdão nº 1.603 (TCU, 2008) e do Levantamento de Governança de TI (TCU, 2010), apontou uma série de deficiências, inclusive no que tange a gestão de riscos.

Preocupada com essas questões, a Coordenação de Gestão de Tecnologia da Informação da Fiocruz tem trabalhado na consolidação de políticas para a elevação de sua governança de TI na instituição. No entanto, para que seja possível avançar na elaboração de modelos corporativos de gestão de riscos de TI, faz-se necessário conhecer de forma prévia o nível de maturidade da instituição em gestão de riscos, permitindo esboçar um diagnóstico e definir adequadamente os próximos passos para a sua contínua evolução.

1.3. Descrição do Problema

Tendo em vista o cenário descrito nos capítulos anteriores e o contexto atual da organização, é possível descrever os problemas associados a esta pesquisa, da seguinte forma:

a. Variedade de modelos de maturidade, não alinhados entre si, dificultando uma escolha;
b. Desconhecimento de critérios para a escolha de um modelo de maturidade em gestão de riscos de TI;
c. Ausência de instrumentos adequados à coleta de dados e avaliação prática do nível de maturidade em gestão de riscos de TI na Fiocruz;

1.4. Objetivos

1.4.1. Objetivo Geral

Propor uma solução para avaliação de maturidade de gestão de riscos de TI a partir da escolha de um modelo de maturidade, definindo instrumento (s) e especificando requisitos para construção de um sistema computacional para apoio ao processo de avaliação.

1.4.2. Objetivos específicos

1) Realizar um estudo comparativo entre modelos de maturidade, tais como: *frameworks*, modelos acadêmicos e norma de referência;

2) Selecionar, junto aos modelos estudados, um modelo de maturidade cujos aspectos melhor atendam, em parte ou íntegra, as expectativas da organização no que se refere à gestão de riscos de TI;
3) Propor um instrumento de coleta e avaliação de maturidade em gestão de riscos de TI, especificando os requisitos funcionais para a construção de uma ferramenta automatizada para apoio ao processo de avaliação de maturidade em gestão de riscos de TI e aplicação do instrumento proposto em uma unidade de TI da organização para sua validação.

1.5. Justificativa

A Coordenação de Gestão de Tecnologia da Informação (CGTI) é a área central de TI da Fiocruz, responsável pelas políticas institucionais de TI e pelos projetos estruturantes da área na instituição. Desde que foi constituída em 2010, a CGTI tem empregado a gestão de riscos por entender ser esta uma prática importante no processo de governança de TI. Nestes quatro anos foi possível definir os contextos internos e externos, estrutura interna, realizar o mapeamento do processo, definir métodos e critérios de avaliação e implantar ferramenta de apoio ao processo de gestão de riscos.

No entanto, apesar de seus esforços, não existe ainda um modelo em nível institucional que evidencie e sustente a prática de gestão de riscos de TI, permitindo não apenas uma definição metodológica, mas também a disseminação da cultura de gestão de riscos de TI e a integração e cooperação entre as outras quinze áreas de TI das unidades da Fiocruz.

Um modelo único em gestão de riscos de TI permitiria definir métodos, critérios, ferramentas e técnicas, que produzissem resultados padronizados, diminuindo custos e preparando as áreas de TI para um crescimento com riscos conhecidos e adequadamente tratados. No entanto, antes de desenvolver esse modelo, é desejável conhecer a capacidade atual das áreas de TI da Fiocruz em gerir riscos de tecnologia da informação, de forma a orientar a construção de um modelo adequado ao seu nível de maturidade. Hoje, não se sabe ao certo quais áreas de TI realizam atividades de gestão de riscos, tampouco sua capacidade na execução dessas atividades.

Embora existam diversos modelos que permitam a uma organização avaliar seu nível de maturidade, estes se diferem na sua aplicação. Alguns estão voltados para a governança corporativa, outros para a governança em TI. Existe ainda norma internacional que trata da avaliação de maturidade com foco em processos e modelos acadêmicos genéricos. Assim, o trabalho se propõe a fazer uma revisão

dos modelos de maturidades existentes e que possam ser aplicados ao escopo da gestão de riscos de TI, propondo a construção de um instrumento de avaliação de maturidade a partir da escolha de um dos modelos, aplicando-o a fim de validar seu método. Dessa forma, espera-se que o trabalho a ser desenvolvido possa trazer contribuições como:

a) Auxiliar a organização no aumento da sua capacidade de gerir riscos;
b) Escolher o modelo mais adequado para aplicação na instituição em um escopo ampliado;
c) Servir como referência para futuros trabalhos acadêmicos sobre o tema;
d) Permitir que organizações similares adotem o mesmo modelo para obtenção da maturidade de forma sistematizada, permitindo assim a comparação dos resultados (*benchmarking)* entre organizações;
e) Promover a melhoria do processo de gestão de riscos em TI na instituição.
f) Alinhar as iniciativas em gestão de riscos ao planejamento estratégico da instituição e ao programa GesPública;

Capítulo 2

Revisão de Literatura

2.1. Conceitos

2.1.1. Risco

O conceito de risco está presente na rotina das pessoas e organizações. Muitas das vezes isso é feito de forma automática, sem que as pessoas se deem conta do que estão fazendo. No entanto, lidar com riscos exige mais que decisões intuitivas e implícitas; "Exige uma gestão ativa de riscos em bases sistemáticas, holísticas e integradas" (HILL, 2006).

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" (HOLANDA, 2004). A Norma ISO Guia 73 define o termo risco como "o efeito da incerteza nos objetivos" (ABNT, 2009a). Essas incertezas não são necessariamente negativas. 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'" (IBGC, 2007).

Para o Departamento de Segurança da Informação e Comunicações (DSIC), risco de segurança da informação pode ser definido como:

> Potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais

> ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização (DSIC, 2013, p. 3).

Segundo Vargas (2009) o estudo do risco teve sua origem no renascimento quando as pessoas se libertaram das restrições do passado e passaram a desafiar crenças consagradas, abrindo caminho para descoberta do mundo e exploração de recursos. Desde então o risco tem sido objeto de estudo por nomes como o matemático Blaise Pascal (para decifrar o enigma proposto por Paccioli), Pierre de Fermat (teoria das probabilidades), Gottfried von Leibniz (retorno dos eventos), Daniel Bernoulli (lei dos grandes números e amostragem estatística), Thomas Bayes (teorema de Bayes) até chegar à gestão de riscos moderna, estudada e aperfeiçoada após a Segunda Guerra Mundial por pesquisadores como Markowitz, Lintner, Treynor, Sharpe e Mossin (DIONNE, 2013).

2.1.2. Gestão de riscos

A Norma ISO Guia 73, que define o vocabulário para a gestão de riscos, descreve o termo como "atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos" (ABNT, 2009a). Para Silveira (2010) a gestão de riscos é uma das funções primordiais dos conselhos de administração dentro de um processo de governança corporativa.

Segundo Elmaallam & Kriouile (2011), 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" (RAMOS, 2008, p. 43). É possível encontrar diversas descrições para o termo gestão de riscos, porém, todas traduzem de forma similar o seu significado, como podemos ver nas definições abaixo extraídas de organizações acadêmica, governamental e de mercado, respectivamente:

> 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 (SEI, 2010).

> 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 (DSIC, 2013, p. 3).

> Um processo conduzido em uma organização [...] 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 (COSO, 2007).

2.1.3. Processo de gestão de riscos

Outro conceito importante é o 'processo de gestão de riscos' apresentado pela ISO 31000 e definido como:

> 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 (ABNT, 2009c).

O processo de gestão de riscos descrito na norma ISO 31000 é apresentado a seguir:

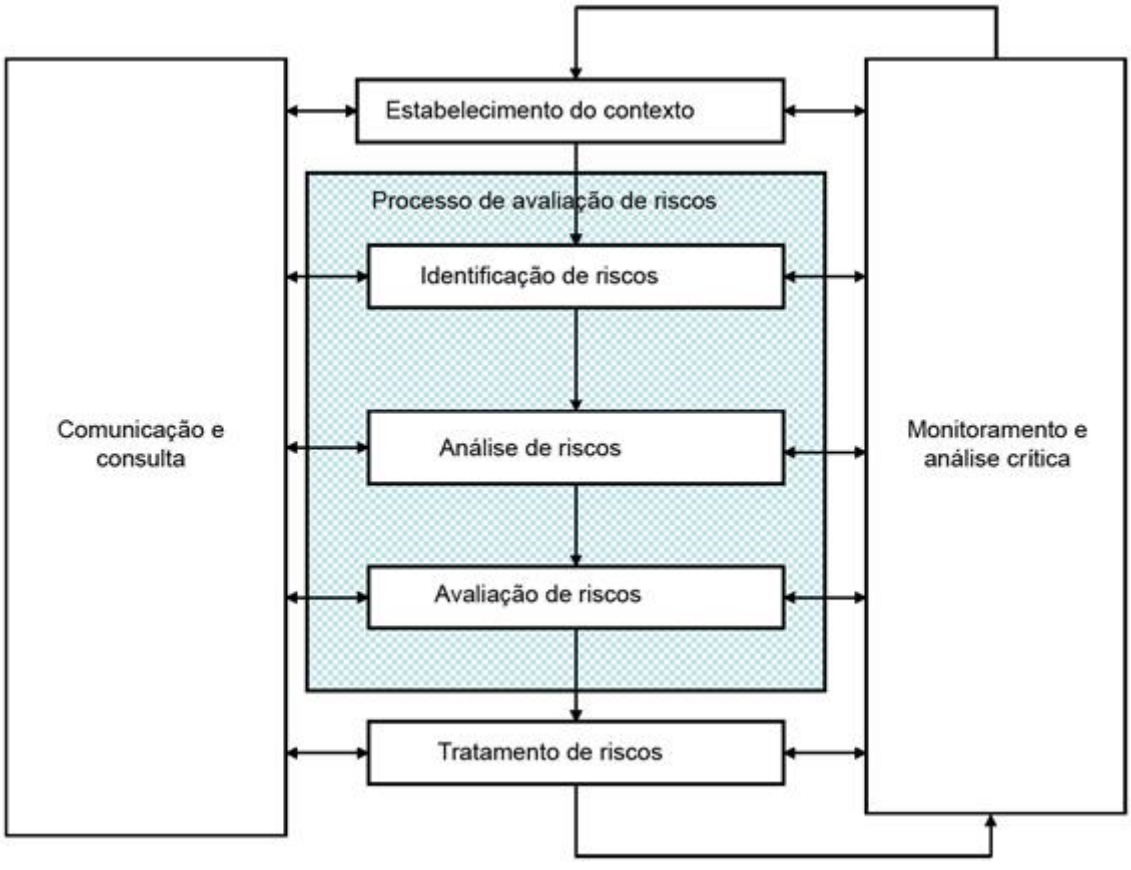


Figura 2: Processo de Gestão de Riscos (ABNT, 2009c)

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. 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 durante todo o ciclo do processo de gestão de riscos.

2.1.4. 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. O Instituto Brasileiro de Governança Corporativa – IBGC define Governança Corporativa como:

> "O sistema pelo qual as organizações são dirigidas, monitoradas e incentivadas [...]. As boas práticas de Governança Corporativa convertem princípios em recomendações objetivas, alinhando interesses com a finalidade de preservar e otimizar o valor da organização[...]" (IBGC, 2009)

Para Silveira (2010), governança corporativa é definida como o conjunto de mecanismos que visam fazer com que as decisões corporativas sejam sempre tomadas com a finalidade de 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 desempenho de monitoramento são determinados" (OECD, 2004). A Norma ISO/IEC 38500, por sua vez, define governança como "o sistema pelo qual as organizações são dirigidas e controladas" (ABNT, 2008d).

A 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 (2006) 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" (Weill & Ross, 2006, p. 14).

2.1.5. Maturidade

Outro termo importante utilizado neste trabalho é "maturidade". O dicionário Aurélio apresenta como definição para maturidade: perfeição, excelência, primor (HOLANDA, 2004). Segundo Crawford (2007), até poucos anos atrás, o conceito de maturidade era raramente usado para descrever o estado de eficácia de uma organização na realização de determinadas tarefas. Hoje, este conceito está sendo cada vez mais utilizado para mapear os caminhos lógicos para melhorar serviços de uma organização, ideia reforçada por Caralli (2011) que diz ser possível encontrar diversos modelos de maturidade que podem ajudar a organização a desenvolver um caminho para melhoria de seus serviços.

O termo também pode ser entendido como a medida de eficiência de um processo através da avaliação de critérios de comparação de uma referência interna da empresa (ELMAALLAM & KRIOUILE, 2011). Os mesmos autores ressaltam que as companhias que querem se proteger e se desenvolver de forma sólida, devem implementar um processo eficaz de gestão de riscos, submetendo-o a uma avaliação contínua por meio de um modelo de maturidade apropriado.

De acordo com a Protiviti (2006a, p. 2) – empresa global de consultoria e auditoria interna – para a organização promover a maturidade de gestão de risco é necessário identificar e fechar lacunas para o nível desejado, através da adoção de um processo evolutivo de maturidade em gestão de riscos (Protiviti, 2006b, p. 84).

Ao analisar a gestão de riscos como um processo é possível aplicar os conceitos contidos no relatório técnico da ABNT ISO/IEC TR 15504-7, que trata da avaliação de processos com vistas à "maturidade organizacional", que é descrito como "o quanto uma organização implementa de forma consistente processos em um escopo definido que contribuem para o atendimento das metas atuais e projetadas de negócio da organização" (ABNT, 2009b).

Outro conceito importante descrito nesta norma é o "nível de maturidade", definido como "um ponto na escala ordinal de maturidade organizacional que caracteriza a maturidade da organização em um escopo do modelo de maturidade organizacional utilizado" (ABNT, 2009b).

Para o *Software Engineering Institute* (2010) um modelo de maturidade fornece elementos para a melhoria de processos de uma organização e descreve um caminho de melhoria evolutiva desde processos imaturos até processos maduros, disciplinados, com qualidade e eficácia melhoradas.

Assim, é possível entender 'maturidade em gestão de riscos' como a indicação do nível de capacidade atual de uma organização em executar um processo

de gestão de riscos, descrevendo não somente sua situação a atual, mas também os caminhos necessários para o alcance da excelência a partir das boas práticas de mercado.

2.2. Modelos de Maturidade

É possível observar que as organizações têm adotado práticas de gestão de riscos, porém, não se observa com frequência organizações implementando métodos para aferição da maturidade das suas práticas em gestão de riscos. Shahzad e Safvi (2010, p. 110) afirmam que "organizações que tem alcançado um nível de maturidade mais elevado podem melhor evitar riscos em suas fases iniciais".

Brito (2011), a partir de uma abordagem de gestão de riscos, traça um levantamento e diagnóstico de maturidade da governança da segurança da informação na administração pública federal. Santos Neto (2007), apresenta uma proposta de modelo de maturidade para gerenciamento de riscos com foco em projetos. Seu modelo de maturidade se propõe a avaliar as atitudes da organização em relação ao gerenciamento de riscos e o seu grau de avanço ao longo dos projetos que executa.

Hillson (1997) apresenta o RMM (*Risk Maturity Model)*, um modelo de maturidade em gestão de riscos para avaliar o nível atual de maturidade, identificar metas realistas para sua melhoria e elaborar planos de ação para desenvolver e aperfeiçoar a sua capacidade de risco. Elmaallam & Kriouile (2011) fazem uma abordagem comparativa entre diversos modelos, entre eles o RMMM (Risk Management Maturity Model), desenvolvido pela *INCOSE Risk Management Working Group* como um modelo simplificado do RMM. Silva (2012) apresenta um modelo de maturidade baseado em formação de valor das organizações, cuja estrutura permite que o modelo seja adaptado e aplicado a qualquer processo de uma organização.

Alguns *Frameworks* de mercado também trazem inseridos em seus contextos modelos maturidade. Os mais conhecidos são o *Control Objectives for Information and related Technology* – COBIT (ITGI), *Entreprise Risk Management – ERM – Integrated Framework* (COSO), *Capability Maturity Model Integration – CMMI* (SEI), entre outros.

Com diversos modelos de maturidade à disposição, qual deles seria mais indicado para aplicação em uma organização diante do contexto apresentado? Alguns modelos são propostas acadêmicas, outros, *Frameworks* consagrados pelo mercado. É comum encontrar modelos que fazem uso da estrutura de outros, diferenciando-se apenas no foco de aplicação.

É assim com o ERM e COBIT, que utilizam o *Capability Maturity Model* – CMM do SEI para avaliação da maturidade. O Modelo apresentado por Silva (2012) utiliza conceitos de classificação dos tipos de ativos de uma organização similares àqueles apresentados pela Protiviti em relação ao ERM. O RMMM da INCOSE toma como base o modelo descrito por Hillson, o RMM. Apesar de suas aplicações serem diferentes (governança corporativa, governança de TI e desenvolvimento de software), seus modelos de avaliação de maturidade apresentam certo grau de similaridade.

Cabe aqui uma ressalva quanto ao domínio de aplicação do modelo de maturidade. O relatório técnico da ABNT ISO/IEC TR 15504-7 orienta que, na escolha de um modelo de maturidade, quando a organização desejar conduzir uma avaliação em uma área que não é representativa do seu domínio normal, deve-se tomar cuidado para que o modelo escolhido seja aplicável (ABNT, 2009b).

Assim, para realizar uma escolha consciente, foram selecionadas algumas propostas que serão submetidas a uma análise comparativa de suas características. A seguir é apresentada uma breve revisão dos modelos selecionados.

2.2.1. Capability Maturity Model Integration – CMMI

O *Capability Maturity Model Integration* – CMMI (Modelo Integrado de Maturidade e de Capacidade) é um modelo de maturidade para melhoria de processo. Seu objetivo é auxiliar as organizações na melhoria de seus processos de desenvolvimento e manutenção de produtos e serviços, através das melhores práticas associadas a atividades, que cobrem o ciclo de vida do produto desde a concepção até a entrega e manutenção (SEI, 2010).

O CMMI surgiu para combinar outros CMMs existentes. Sua estrutura fornece os elementos essenciais de um processo efetivo, cobrindo várias disciplinas e traçando um caminho de melhoria evolutiva do processo.

A fim de desenvolver e manter produtos e serviços de qualidade, o modelo foi desenvolvido a partir de três dimensões críticas nas quais as organizações devem se concentrar:

a) Pessoas;
b) Procedimentos e métodos;
c) Ferramentas e equipamentos;

A coesão entre essas três dimensões é feita através dos processos de negócio da organização, que fornece os elementos necessários para a otimização de recursos, maximização da produtividade e maior competitividade.

O CMMI oferece duas abordagens distintas: contínua e por estágios. A abordagem contínua permite à organização melhorar de forma incremental os processos correspondentes a uma ou mais áreas de processo individualmente selecionadas pela organização. Já a abordagem por estágios permite que as organizações melhorem um conjunto de processos inter-relacionados, tratando sucessivos conjuntos de áreas de processos de forma incremental.

Para a representação contínua, utiliza-se o termo "nível de capacidade" e para a representação por estágios "nível de maturidade" (SEI, 2010). A tabela a seguir demonstra uma comparação entre os níveis de capacidade e maturidade do CMMI:

Tabela 1: Níveis de maturidade e capacidade do CMMI (SEI, 2010).

Nível	**Níveis de Maturidade Representação por Estágios**
Nível 1	Inicial
Nível 2	Gerenciado
Nível 3	Definido
Nível 4	Gerenciado quantitativamente
Nível 5	Otimizando

Para a progressão entre os níveis de maturidade o CMMI define um conjunto práticas específicas e genéricas associadas às áreas de processo. Para se alcançar um nível, todos os requisitos do nível anterior devem ter sido cumpridos.

A área de processo pode ser definida como "conjunto de práticas relacionadas em uma área que, quando implementadas conjuntamente, satisfazem a um conjunto de metas consideradas importantes para a realização de melhorias naquela área" (SEI, 2010).

A gestão de riscos é uma das vinte e quatro áreas de processo do CMMI-SRV, sendo esta a área de processo selecionada para o estudo comparativo. Segundo o CMMI-SVC o objetivo desta área de processo é:

> Fornecer subsídios para identificar potenciais problemas antes que ocorram, de forma que atividades de tratamento de riscos possam ser planejadas e colocadas em prática quando necessário (ao longo da vida do produto ou do projeto) para mitigar impactos indesejáveis que comprometam a realização dos objetivos (SEI, 2010).

2.2.2. Control Objectives for Information and related Technology – COBIT 4.1

O *Control Objectives for Information and related Technology* – COBIT é um *Framework* desenvolvido pelo *IT Governance Institute* – ITGI que fornece boas práticas – que são o consenso de especialistas – através de uma estrutura lógica e gerenciável para garantir que a área de TI suporte adequadamente os objetivos de negócio da instituição. O COBIT foi desenvolvido de forma que estivesse alinhado com o COSO, um modelo de governança e gerenciamento de riscos muito utilizado pelo mercado.

Para que as organizações possam aperfeiçoar o uso dos recursos de TI, os dirigentes precisam entender o estágio atual da sua arquitetura de TI a fim de

identificar que caminho deverá seguir. Assim, o COBIT busca um alinhamento entre os objetivos de negócios e os objetivos de TI da organização, através de modelos de maturidade e métricas que possam mediar sua eficácia e identificar responsabilidades dos donos de processos de negócios e de TI.

O COBIT 4.1 utiliza um modelo de maturidade (para avaliação de performance e capacidade dos processos de TI) derivado do *Capability Maturity Model* (CMM) desenvolvido pelo *Software Engineering Institute* (SEI). Para definir e avaliar os resultados e performance dos processos, os objetivos e métricas foram baseados no *Balanced Scorecard,* desenvolvido por Robert Kaplan e David Norton.

O COBIT 4.1 trabalha ainda com o conceito de 'áreas de foco', que pode ser entendido como tópicos os quais os dirigentes precisam estar atentos. Dentre as cinco áreas de foco existentes está a área de gestão de riscos.

A *Framework* COBIT 4.1 provê um modelo constituído por 34 processos, agrupados em 4 domínios inter-relacionados, que se alinham ás áreas responsáveis por planejar, construir, executar e monitorar, de forma a prover uma visão total da área de TI (ITGI, 2007).

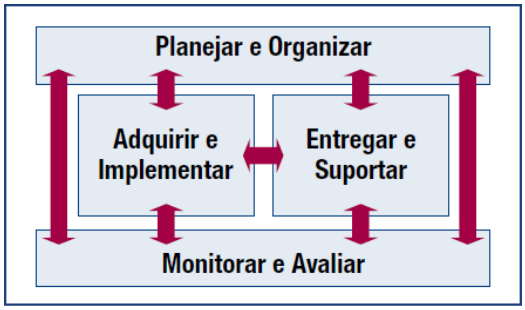


Figura 3: Domínios inter-relacionados do COBIT 4.1 (ITGI, 2007)

O domínio Planejar e Organizar (PO) cobre os aspectos referentes as estratégias e táticas necessárias para a TI contribuir para o alcance dos objetivos de negócio. O domínio Adquirir e Implementar (AI) se preocupa com as soluções de TI que precisam ser desenvolvidas, adquiridas ou implementadas para integração ao processo de negócios necessários para a execução das estratégias de TI. O domínio Entregar e Suportar (DS), refere-se a entrega e gerenciamento dos serviços solicitados. Por fim, o domínio Monitorar e Avaliar (ME) diz respeito a avaliação dos processos a fim de assegurar a qualidade e a aderência aos requisitos de controle. A tabela a seguir descreve os quatro domínios do COBIT 4.1 e seus respectivos processos:

Tabela 2: Domínios e processos do COBIT 4.1 (ITGI, 2007)

Domínio	Processo
Planejar e Organizar	PO1 Definir um Plano Estratégico de TI
	P02 Definir a Arquitetura da Informação
	PO3 Determinar o Direcionamento Tecnológico
	PO4 Definir os Processos, Organização e os Relacionamentos de TI
	PO5 Gerenciar o Investimento de TI
	PO6 Comunicar as Diretrizes e Expectativas da Diretoria
	PO7 Gerenciar os Recursos Humanos de TI
	PO8 Gerenciar a Qualidade
	PO9 Avaliar e Gerenciar os Riscos de TI
	PO10 Gerenciar Projetos
Adquirir e Implementar	AI1 Identificar Solução Automatizadas
	AI2 Adquirir e Manter Software Aplicativo
	AI3 Adquirir e Manter Infraestrutura de Tecnologia
	AI4 Habilitar Operação e Uso
	AI5 Adquirir Recursos de TI
	AI6 Gerenciar Mudanças
	AI7 Instalar e Homologar Soluções e Mudanças
Entregar e Suportar	DS1 Definir e Gerenciar Níveis de Serviços
	DS2 Gerenciar Serviços de Terceiros
	DS3 Gerenciar Capacidade e Desempenho
	DS4 Assegurar Continuidade de Serviços
	DS5 Assegurar a Segurança dos Serviços
	DS6 Identificar e Alocar Custos
	DS7 Educar e Treinar os Usuários
	DS8 Gerenciar a Central de Serviço e os Incidentes

Domínio	Processo
	DS9 Gerenciar a Configuração
	DS10 Gerenciar os Problemas
	DS11 Gerenciar os Dados
	DS12 Gerenciar o Ambiente Físico
	DS13 Gerenciar as Operações
Monitorar e Avaliar	ME1 Monitorar e Avaliar o Desempenho
	ME2 Monitorar e Avaliar os Controles Internos
	ME3 Assegurar a Conformidade com Requisitos Externos
	ME4 Prover a Governança de TI

Observa-se que o domínio "Planejar e Organizar" é constituído por dez processos, sendo um deles o processo 'Avaliar e Gerenciar os Riscos de TI'. Os processos do COBIT estão descritos de forma a se alinhar aos objetivos de TI que suportam os objetivos de negócio da organização. Para fins deste trabalho será considerado apenas o processo PO9 - Avaliar e Gerenciar os Riscos de TI - foco do estudo de maturidade proposto. Segundo o ITGI (2007) o processo Avaliar e Gerenciar os Riscos de TI (PO9) visa:

> Criar e manter uma estrutura de gestão de risco. Esta estrutura documenta um nível comum e acordado de riscos de TI, estratégias de mitigação e riscos residuais. Qualquer impacto em potencial nos objetivos da empresa causado por um evento não planejado deve ser identificado, analisado e avaliado. Estratégias de mitigação de risco devem ser adotadas para minimizar o risco residual a níveis aceitáveis. O resultado da avaliação deve ser entendido pelas partes interessadas e expresso em termos financeiros para permitir que as partes interessadas alinhem o risco a níveis de tolerância aceitáveis.

Para o processo PO9 são definidos ainda um conjunto de seis controles gerenciais que devem ser considerados pela área de TI na implementação do processo, de forma a prover uma razoável garantia de que os objetivos de negócio possam atingidos e que eventos indesejáveis possam ser prevenidos, ou ainda detectados e corrigidos (ITGI, 2007). Os objetivos de controles do processo PO9 são:

- PO9.1 Alinhamento da gestão de riscos de TI e de Negócios;
- PO9.2 Estabelecimento do Contexto de Risco;
- PO9.3 Identificação de Eventos;
- PO9.4 Avaliação de Risco;
- PO9.5 Resposta ao Risco;
- PO9.6 Manutenção e Monitoramento do Plano de Ação de Risco;

O modelo de maturidade do COBIT permite que a organização seja classificada em uma escala de maturidade que vai do inexistente ao otimizado. Diferentemente do enfoque apresentado pelo CMMI, o modelo de maturidade do COBIT 4.1 permite traçar um perfil da organização demonstrando sua maturidade em cada nível, ou seja, não é necessário atingir um nível anterior para alcançar o próximo. A seguir é apresentada a escala de maturidade sugerida pelo COBIT 4.1

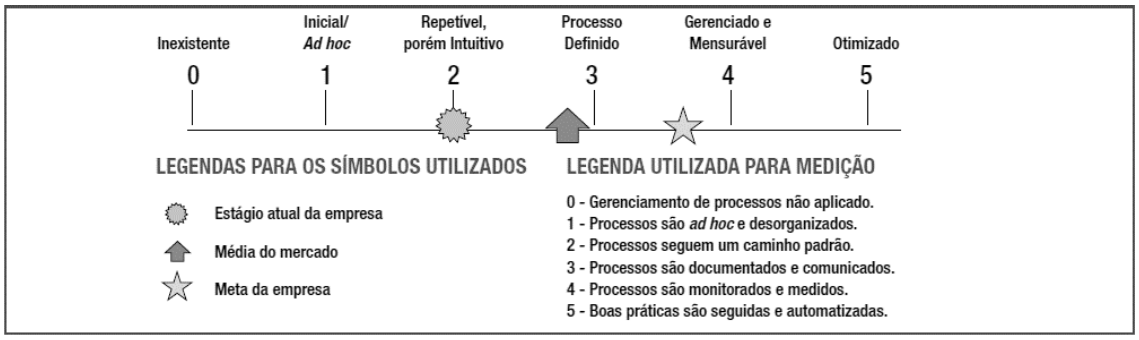


Figura 4: Representação gráfica do modelo de maturidade do COBIT (ITGI, 2007)

Como é possível observar, o modelo de maturidade desenvolvido pelo COBIT 4.1 permite à organização representar em uma mesma escala:

i. O estágio atual de performance da empresa – Onde a empresa está hoje;
ii. O estágio atual do mercado – A comparação;
iii. A meta de aprimoramento da empresa – Onde a empresa quer estar;
iv. O caminho de crescimento entre o "como está" e "como será";

Originalmente, o COBIT 4.1, tinha seu modelo de maturidade derivado do *Capability Maturity Model* (CMM) desenvolvido pelo *Software Engineering Institute* (ITGI, 2007). Em 2011 foi lançado o documento COBIT *Process Assessment Model* – PAM, que alinha o COBIT 4.1 a norma internacional ISO/IEC 15504-2, abandonando, por conseguinte, o modelo CMM (ISACA, 2011a). O PAM faz parte do programa de avaliação do COBIT denominado COBIT *Assessment Programme*.

Esse programa de avaliação do COBIT foi projetado para fornecer às organizações uma metodologia repetível, confiável e robusta para avaliar a capacidade de seus processos de TI e são normalmente utilizadas como parte de um programa de melhoria a partir de sua capacidade atual para alcançar uma meta de melhoria com base em requisitos de negócios (ISACA, 2011b).

Segundo o ISACA (2011a), embora as duas abordagens – CMM e ISO/IEC 15504 – utilizem o mesmo número de níveis de maturidade, o novo modelo de avaliação apresenta uma abordagem mais robusta e confiável, a fim de prover resultados mais consistentes. A avaliação detalhada do processo ocorre no nível 1 (com base no COBIT) e os demais níveis de capacidade na norma ISO/IEC 15504, que prescrevem resultados genéricos, práticas base e produtos de trabalho, a serem avaliados nos níveis de capacidade superiores.

2.2.3. Control Objectives for Information and related Technology – COBIT 5

Em 2012 foi lançada uma nova versão do *Framework* COBIT, com profundas mudanças, inclusive no que tange o modelo de maturidade. A versão anterior do COBIT (4.1) utilizava o *Capability Maturity Model* (CMM) do *Software Engineering Institute* como referência para seu modelo de maturidade. Em sua versão 5 o modelo de maturidade passa a se basear na família ISO/IEC 15504 - *Information Technology – Process Assessment*. O COBIT 5 utiliza novos conceitos em sua estrutura, apresentados como princípios e capacitadores. Apesar de continuar com seis níveis de maturidade, o novo modelo de maturidade do COBIT 5 vai do "processo incompleto" ao "processo em otimização".

Nesta nova versão um nível de capacidade só pode ser alcançado quando todos os atributos do nível anterior tiverem sido concluídos (ISACA, 2012b). A família de produtos do COBIT 5 inclui, além da *Framework* em si, o "*COBIT 5 enabler guides*" (onde os capacitadores de governança e gerenciamento são discutidos em detalhe) e guia profissionais, entre eles o "*COBIT 5 for Risk*", com orientações sobre o gerenciamento de riscos, mas que ainda se encontra em desenvolvimento (ISACA, 2012c).

2.2.4. Entreprise Risk Management – ERM

O *Enterprise Risk Management – Integrated Framework* é um modelo de gerenciamento de riscos corporativos desenvolvido pelo *Committee of Sponsoring Organization of the Treadway Commission* (COSO) com a finalidade de proporcionar as diretrizes para a evolução e aprimoramento do gerenciamento de

riscos dos procedimentos para sua análise, servindo como base para que uma organização possa determinar se o gerenciamento de riscos está sendo eficaz, ou ao contrário, o que necessita para se tornar eficaz.

A implementação da estrutura do ERM suporta e melhora a consciência do risco em todos os níveis, desde o nível estratégico ao operacional (BLATTNER & CIORCIARI, 2008). O modelo COSO sugere o uso de uma matriz tridimensional, representado na figura abaixo:

Figura 5: Matriz de relacionamento (COSO, 2007)

A estrutura da matriz tridimensional sugere um relacionamento entre os objetivos da organização, os componentes do gerenciamento de riscos corporativos e as unidades de uma organização (COSO, 2007).

O ERM permite que as organizações melhorem a maturidade das suas capacidades de gerenciar riscos prioritários, aumentem suas chances de sucesso e protejam o valor da empresa a partir de três perspectivas:

i. Estabelecer uma vantagem competitiva sustentável;
ii. Otimizar o custo de gerenciamento de risco;
iii. Melhorar a performance da gestão empresarial.

CONTÍNUO	ATRIBUTOS DE CAPACIDADE	MÉTODO DE REALIZAÇÃO
Otimizando	(*Feedback* contínuo) Gerenciamento de riscos como uma fonte de vantagem competitiva	• Aumento da ênfase na exploração de oportunidades • Processos "melhor da classe" • Conhecimento acumulado e compartilhado
Gerenciado	(Quantitativo) Riscos medidos/gerenciados quantitativamente e toda empresa agregada	• Metodologias / análises rigorosas de medição • Debate intensivo sobre questões como premiação e risco
Definido	(Qualitativo/Quantitativo) Políticas, processos e padrões definidos e institucionalizado	• Processos uniformemente aplicados através da organização • Elementos restantes da infraestrutura local • Metodologias rigorosas
Repetível	(Intuitivo) Processo estabelecido e repetível. Dependência contínua de pessoas	• Linguagem comum • Pessoas de qualidade associadas • Tarefas definidas • Elementos de infraestrutura inicial
Inicial	(*Ad Hoc* / Caótico) Dependente de atitudes heroicas; Capacidade institucional deficiente	• Tarefas não definidas • Depende de iniciativas • "basta fazê-lo" • Dependência de pessoa chave

Figura 6: Nível de maturidade do ERM (Protiviti, 2006a).

O Guia de implementação do ERM desenvolvido pela empresa Protiviti apresenta um modelo de maturidade para determinar a necessidade de melhorias no gerenciamento de riscos. Esse modelo foi desenvolvido com base no modelo CMM do *Software Engeering Institute*, representado por cinco estágios que vai do inicial ao otimizado.

2.2.5. Formação de valor em sistemas de atividades humanas – FVSAH

O modelo de maturidade proposto por Silva (2012) está baseado em formação de valor em sistemas de atividades humanas – FVSAH. Para Curtis e Carey (2012, p. 7), valor é uma função de risco e retorno, onde cada decisão aumenta, conserva ou deprecia seu valor. Para Boulton et al (2000) o valor das instituições vem se transformando, onde conceitos e ideias tem assumido o lugar de recursos físicos e humanos na produção de produtos e serviços.

O mesmo autor classifica os ativos mais significantes em cinco tipos: físicos, financeiros, cliente, empregado/fornecedor e organização; chamando atenção para

o fato de que esta nova conformação da organização, denominada “nova economia”, traz consigo novos riscos. A mesma classificação é utilizada pela Protiviti (2006a, p. 5-7).

Burgman (2005) propôs uma nova forma de classificação, que evolui a classificação proposta originalmente por Boulton, agrupando-os em ativos tradicionais (físico e monetário) e ativos de capital intelectual (humano, organizacional e relacional). O modelo de maturidade FVSAH usa essa classificação como elemento-chave e vai além, propondo uma matriz de valorização inovadora, pois acrescenta uma visão dos objetos de valor de forma a identificar o que é realizável e o que pode vir a ser uma potencialidade.

Em relação ao termo sistema de atividade humana, encontram-se várias definições: “entidade que mantém sua existência pela interação mútua de suas partes” (BERTALANFFY, 2008) ou “conjunto de elementos conectados que formam um todo, com esse todo tendo propriedades que são dele e não de suas partes” (CHECKLAND, 1999) ou “Conjunto de elementos que interagem para formar um todo integrado” (ROSNAY, 1977).

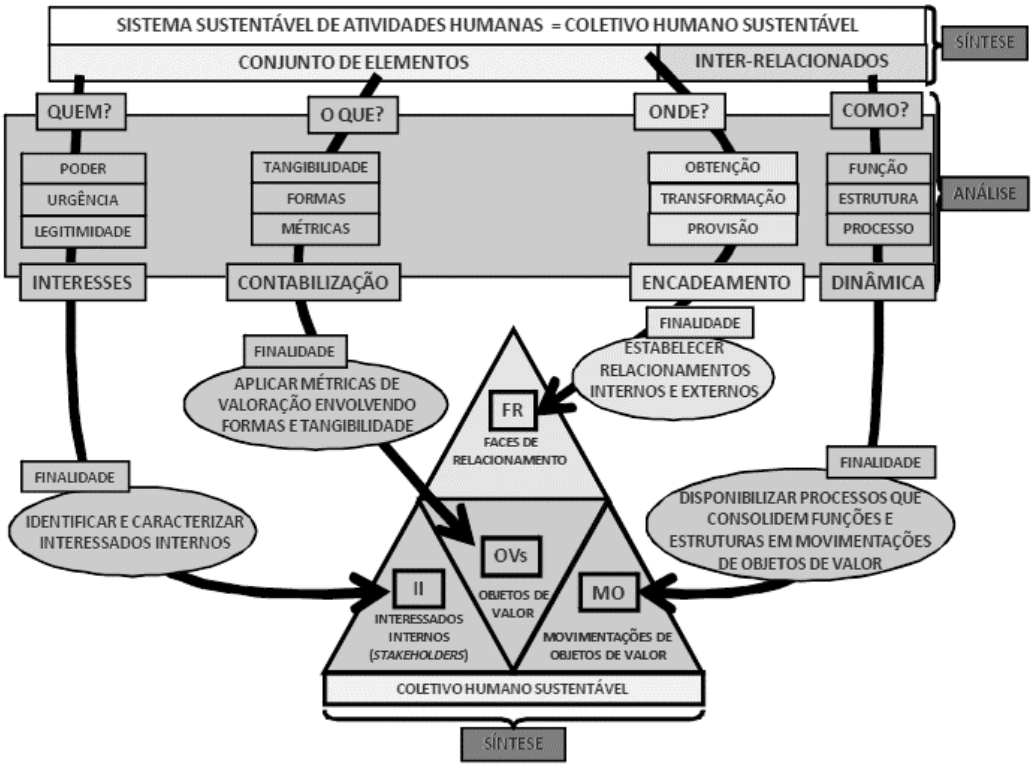


Figura 7: Estrutura constitucional do modelo FVSAH (SILVA, 2012)

A premissa básica deste modelo é que a formação de valor é considerada o propósito maior de qualquer sistema de atividades humanas, englobando tanto a geração e conformação de valor quanto a apropriação desse valor a indivíduos ou

grupos sociais interessados (SILVA, 2012). O modelo FVSAH apresenta cinco níveis de maturidade, sendo o primeiro nível 'funcionamento' e o último 'referência'.

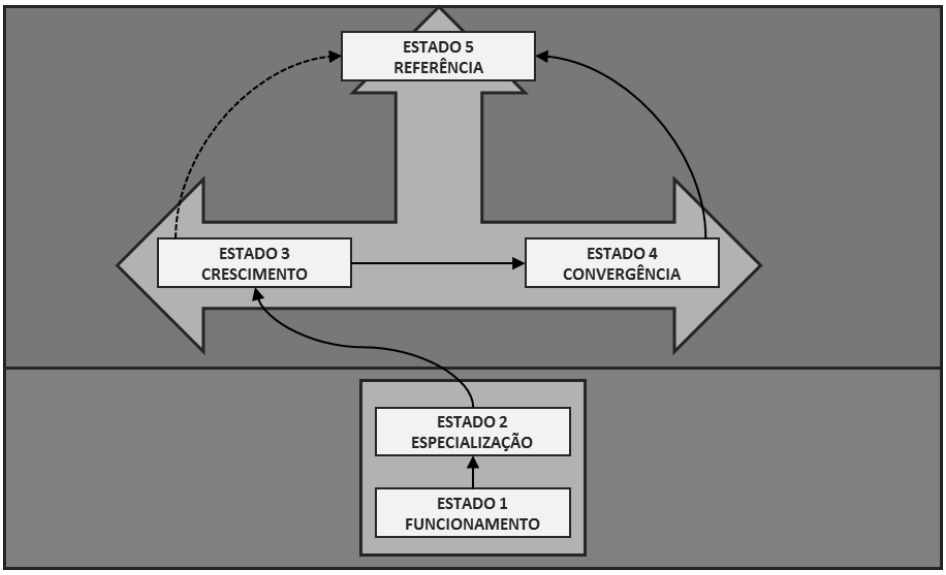


Figura 8: Níveis de maturidade do modelo FVSAH (SILVA, 2012)

Para aplicação do modelo se faz necessário definir os espaços originais de fundação e os espaços de procura, elementos bases para a definição das matrizes de valorização espacial.

MATRIZ DE VALORIZAÇÃO ESPACIAL 1					ITERAÇÃO E INTERAÇÃO			
					FACES/CAMADAS DE RELACIOAMENTO (Espaço Original de Encadeamento)	OBJETOS DE VALOR (Espaço Original de Contabilização)	INTRESSADOS INTERNOS (Espaço Original de Interesses)	MOVIMENTAÇÕES DE OBJETOS DE VALOR (Espaço Original de Dinâmica)
ESTADO 1: NÍVEL DE MATURIDADE 1	SEÇÕES DE ESPAÇO DE VALORIZAÇÃO	ESCOPO	FUNDAÇÃO					
			PROCURA	COESÃO				
				APRENDIZADO				
				QUALIDADE				
				GOVERNANÇA				

Figura 9: Exemplo de matriz de valorização espacial (SILVA, 2012)

Os espaços originais de fundação são compostos por faces/camadas de relacionamento, objetos de valor, interessados internos e movimentações de objetos

de valor. Já os espaços de procura são formados pela coesão, aprendizado, qualidade e governança.

2.2.6. ISO/IEC 15504

A norma ABNT NBR ISO/IEC 15504-2 (tradução da norma internacional ISO/IEC 15504-2), define a estrutura e condições para uma avaliação de maturidade organizacional a partir da avaliação da capacidade de processo ABNT (2008b). A norma descreve os requisitos para

i. Construir modelos de maturidade organizacional;
ii. Realizar uma avaliação de maturidade organizacional;
iii. Verificar conformidade das avaliações de maturidade organizacional;

Segundo a ABNT (2009b) maturidade organizacional é "uma expressão do grau no qual uma organização implementa consistentemente processos em um escopo definido que contribuem para o atendimento de seus objetivos de negócios (correntes ou projetados)". A escala de maturidade da norma ISSO/IEC 15504-2 é exibida a seguir:

Figura 10: Níveis de maturidade da Norma ISO/IEC 15504-2 (ABNT, 2008b)

A escala de maturidade possui seis níveis, onde sua estrutura de medição fornece para a avaliação de capacidade de um processo uma representação crescente, que vai do "incompleto" ao "em otimização" (ABNT, 2008b).

A medição da capacidade é feita com base em um conjunto de atributos de processo, que define uma escala de pontuação, podendo ser: não atingido, parcialmente atingido, amplamente atingido e completamente atingido. Para alcançar um nível de maturidade todos os processos daquele nível e do anterior devem ser alcançados.

2.2.7. Risk Maturity Model - RMM

A *Framework Risk Maturity Model* – RMM proposta por David Hillson [1997] sugere quatro níveis de capacidade: ingênuo, principiante, normalizado e natural.

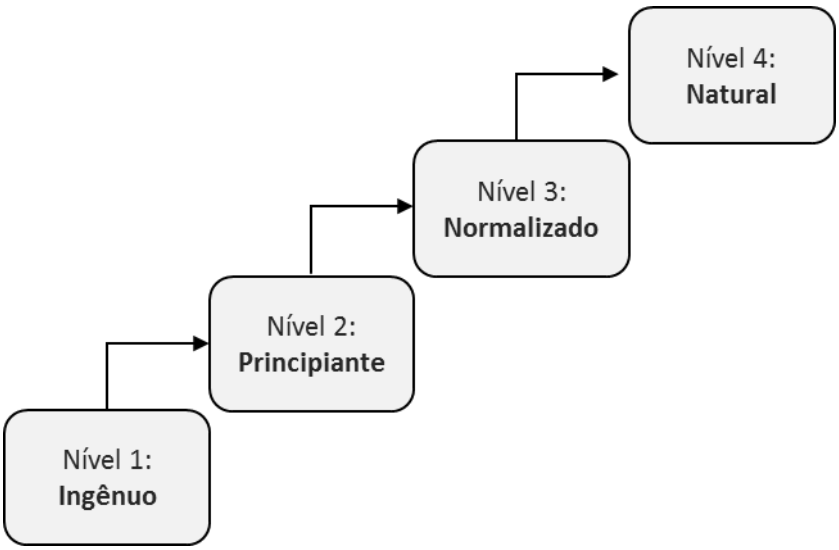


Figura 11: Níveis de maturidade do RMM (Hillson, 1997)

Segundo o autor, reconhece-se que algumas organizações podem não se encaixar perfeitamente nessas categorias, mas os níveis propostos pelo modelo são suficientemente diferentes para acomodar a maioria das organizações de forma não ambígua.

Tabela 3: Relacionamento dos atributos do RMM entre áreas e níveis (Hillson, 1997)

	Nível 1 **Ingênuo**	**Nível 2** **Principiante**	**Nível 3** **Normalizado**	**Nível 4** **Natural**
Definição	Desconhecem a necessidade de gerenciamento de risco. Não existe uma abordagem estruturada para lidar com a incerteza. Processo de gestão reativo e repetitivo. Pouca ou nenhuma tentativa de aprender com o passado ou para se preparar para o futuro.	Experiência com gestão de riscos através de um pequeno número de indivíduos. Nenhuma abordagem genérica estruturada localmente. Consciência dos benefícios potenciais da gestão de risco, mas aplicação ineficaz e sem ganho pleno de benefícios.	Gerenciamento de riscos construído em processos de negócio rotineiros. Gerenciamento de riscos implementado na maioria ou todos os projetos. Processos de genérico de riscos formalizado. Benefícios entendidos em todos os níveis da organização, embora nem sempre sejam consistentemente alcançados.	Cultura na consciência em risco com uma abordagem proativa do gerenciamento do risco em todos os aspectos do negócio. Uso ativo das informações sobre riscos para melhorar os processos de negócio e ganhar vantagem competitiva. Ênfase no gerenciamento de oportunidades (riscos positivos).
Cultura	Sem consciência do risco. Resistente / Relutante em mudar. Tendência a continuar	Processo de risco pode ser visto como uma sobrecarga adicional com benefícios	Aceitação da política de gestão de riscos. Benefícios reconhecidos e esperados. Preparado	Compromisso com a gestão de riscos de cima para baixo (da liderança, por

	Nível 1 **Ingênuo**	**Nível 2** **Principiante**	**Nível 3** **Normalizado**	**Nível 4** **Natural**
	com processo existente.	variáveis. Gerenciamento do risco empregado somente em projetos selecionados.	para comprometer recursos a fim de colher ganhos.	exemplo). Gestão de riscos proativa encorajada e recompensada.
Processo	Não há um processo formal.	Não há um processo genérico formal, embora alguns métodos formais específicos possam estar em uso.	Processo genérico aplicado à maioria dos projetos. Processo formal incorporado ao sistema de qualidade. Alocação de ativos e gestão dos orçamentos de risco em todos os níveis. Alocação de ativos e gestão dos orçamentos de risco em todos os níveis. Necessidade limitada de apoio externo.	Processos de negócio baseados em risco. 'Gestão Total do Risco' transversal a todo o negócio. Atualização regular e frequente dos processos. Métrica das rotinas de risco com comentários consistentes para a melhoria.
Experiência	Não entendimento dos princípios do risco ou linguagem.	Limitado a indivíduos quem possam tiveram um treinamento pequeno ou informal.	Especialistas locais, formalmente treinados em habilidades básicas. Desenvolvimento de processos específicos e ferramentas.	Toda a equipe consciente dos riscos e usando habilidades básicas. Aprendizagem através da experiência como parte do processo. Treinamento externos regulares para aprimorar habilidades.
Aplicação	Não há aplicativos estruturados. Não á recursos dedicados. Não existe ferramentas de risco.	Aplicação inconsistente. Disponibilidade variável de pessoal. Coleção *ad hoc* de ferramentas e métodos.	Rotina e aplicativos consistentes para todos os projetos e recursos entregues. Conjunto integrado de ferramentas e métodos.	Segunda natureza, aplicada para todas atividades. Relatórios de riscos-base para a tomada de decisão. Estado da arte em ferramentas e métodos.

O RMM permite medir a maturidade do risco a partir das quatros áreas (cultura, processo, experiência e aplicação) descritos na tabela 3, onde a transição entre níveis se dá a partir do relacionamento dos atributos dessas áreas com os níveis (HILLSON, 1997). Segundo Hillson, o RMM permite que:

> As organizações referenciem a sua capacidade de risco em quatro níveis de maturidade, a fim de identificar o que precisa ser feito para

> melhorar e desenvolver a sua capacidade de gerenciar riscos. O uso da RMM também vai permitir [...] diagnosticar a situação atual, e ajudar no desenvolvimento de estratégias específicas para o progresso de uma implementação eficaz. (HILLSON, 1997).

Hopkinson (2011b) apresenta uma adaptação do modelo RMM para o processo de gerenciamento de riscos de um projeto, onde os riscos são avaliados a partir de seis perspectivas: projeto das partes interessadas, identificação de riscos, análise de risco, respostas aos riscos, gerenciamento de projetos e cultura de gestão de risco.

O RMM permite uma avaliação global da capacidade de gerenciamento do risco a partir da comparação das seis perspectivas, evidenciando aquela que apresenta o maior risco.

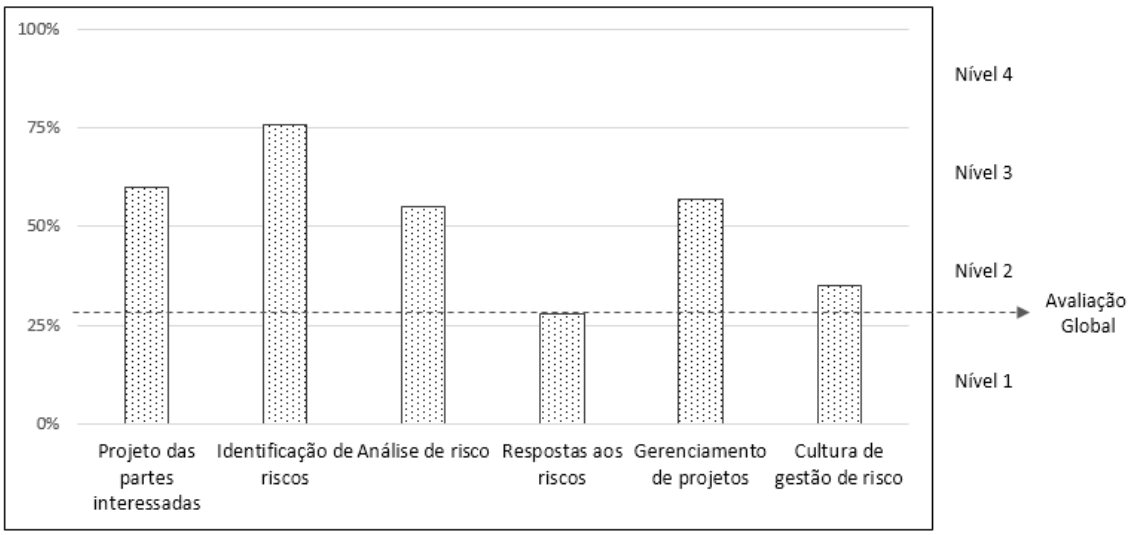


Figura 12: Exemplo de resultados a partir do modelo RMM (Hopkinson, 2011b)

No exemplo da figura 12é possível observar a avaliação de cada uma das perspectivas do modelo, onde a perspectiva 'resposta ao risco' está abaixo da média global.

Capítulo 3

Metodologia

A proposta deste trabalho de dissertação é a realização de um estudo sobre modelos de maturidade que possam ser aplicados no contexto da gestão de riscos de TI. O estudo compreende a realização de um comparativo entre os modelos de maturidade, a definição de critérios para escolha de um modelo de maturidade, a seleção de um modelo de maturidade, a proposição de um instrumento de avaliação com base no modelo de maturidade selecionado, a especificação dos requisitos funcionais para a definição de uma ferramenta de apoio ao processo de avaliação de maturidade e a simulação da aplicação do instrumento de avaliação sugerido para sua validação.

Rehfeldt (1980) diz que a dissertação é a "aplicação de uma teoria já existente para analisar determinado problema". Enquanto trabalho científico, a dissertação, exige metodologia própria, ou seja, sistematização, ordenação e interpretação dos dados (LAKATOS & MARCONI, 2011a). A metodologia é composta por métodos de pesquisa e técnicas de pesquisa, onde os métodos são divididos em métodos amplos e métodos de procedimento.

Foi empregado o método amplo hipotético-dedutivo, onde, segundo Lakatos & Marconi (2011a), a partir de uma hipótese formulada se identifica uma lacuna no conhecimento e pelo processo de inferência dedutiva testa a predição da ocorrência de fenômenos abrangidos pela hipótese.

Em relação ao método de procedimento, este se divide em estratégia da pesquisa e abordagem da pesquisa. Foi utilizada como estratégia de pesquisa a pesquisa-ação, onde, segundo Bryman (1989), o pesquisador e agentes envolvidos nesta trabalham de forma colaborativa no reconhecimento do problema e na proposta de solução. Em relação à abordagem da pesquisa, foram utilizadas as abordagens qualitativa e quantitativa.

Foram utilizadas diversas técnicas, tais como entrevista, pesquisa documental, pesquisa bibliográfica, análise de conteúdo, entrevistas, questionários, medidas de opinião e pesquisa de campo, representadas no diagrama a seguir e descritas conforme os objetivos deste trabalho nos capítulos seguintes.

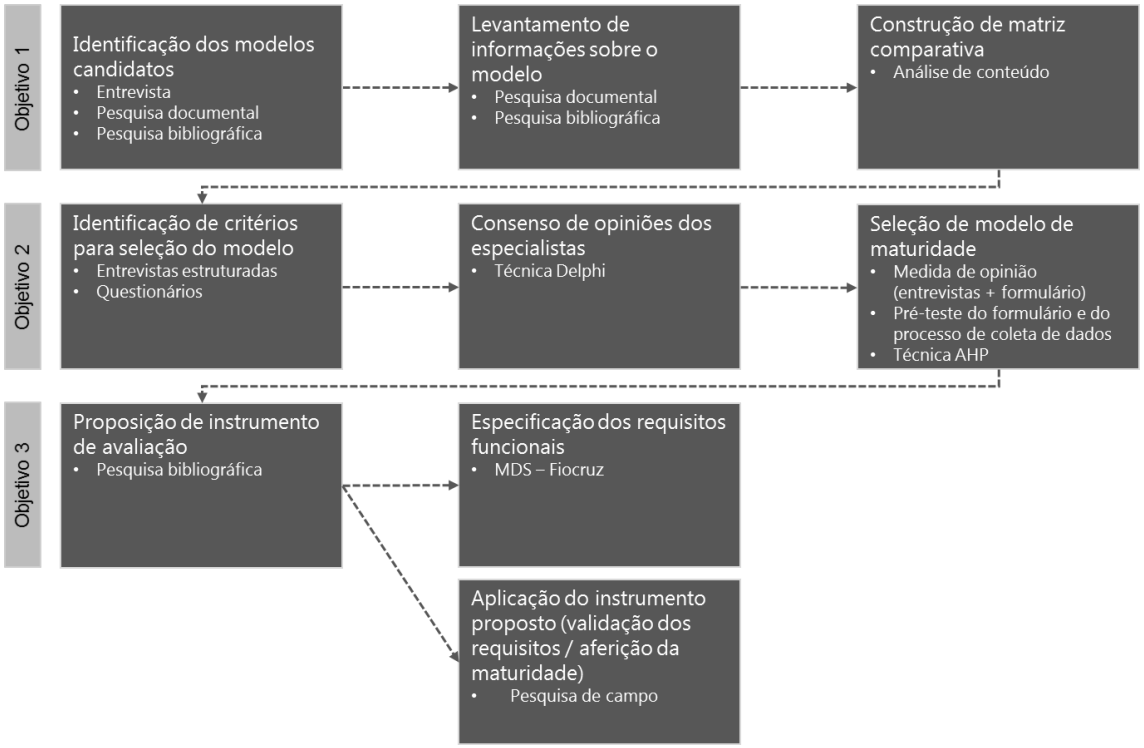


Figura 13: Esquema resumido da metodologia

A figura anterior descreve de forma resumida a metodologia utilizada para o desenvolvimento dos objetivos do trabalho, que será detalhadamente descrita a seguir.

3.1. Estudo comparativo

O primeiro objetivo da pesquisa foi a realização de um estudo comparativo das características dos modelos de maturidade que pudessem ser aplicados à gestão de riscos, com foco na tecnologia da informação. O trabalho se iniciou com a identificação dos modelos candidatos ao estudo proposto. Para isso, foram realizadas entrevistas qualitativas com um grupo de seis pessoas, entre professores e profissionais atuantes na área de gestão de riscos, complementadas por pesquisas do tipo documental e bibliográfica.

Para Lakatos e Marconi (2011a), a entrevista é classificada como uma técnica de observação direta intensiva do processo de documentação direta, cujo objetivo é obter respostas sobre o tema ou problema a investigar, sendo flexível e

aberta, baseados em um guia geral com tema não específico, nas quais o entrevistador tem toda flexibilidade para manipulá-lo. Os mesmos autores classificam as pesquisas documental e bibliográfica como um processo de documentação indireta, onde a técnica de pesquisa documental tem seu foco nas fontes primárias (documento de primeira mão) e a pesquisa bibliográfica nas fontes secundárias (levantamento bibliográfico já publicado).

Uma vez selecionados os modelos de maturidade candidatos, a pesquisa documental e bibliográfica continuou a ser utilizada como técnica para o levantamento de informações sobre os modelos e ainda para verificação quanto a sua adequabilidade ao escopo proposto – gestão de riscos de tecnologia da informação.

Foi realizada ainda uma análise de conteúdo dos documentos de referência através da técnica de observação direta extensiva. Essa técnica é parte do processo de documentação direta e foi utilizada para a construção de uma matriz comparativa, que permitiu a descrição sistemática e objetiva das características dos modelos de maturidade estudados.

3.2. Seleção do modelo de maturidade

O segundo objetivo da pesquisa foi a seleção de um modelo que melhor atendesse aos requisitos de maturidade com foco na gestão de riscos de TI segundo as expectativas da organização. Para a identificação dos possíveis critérios para a seleção de um modelo de maturidade, foram realizadas entrevistas estruturadas (observação direta intensiva) com um grupo seis de profissionais com notório saber na área de gestão de riscos em TI e em modelos de maturidade, oriundos de universidades federais, órgãos do governo federal e empresas de consultoria e auditoria. Devido à distância e disponibilidade de agenda de alguns participantes, foram aplicados questionários para o levantamento de informações.

A entrevista estruturada (ou padronizada) é aquela em que o entrevistador lança mão de um roteiro com perguntas pré-determinadas (LAKATOS E MARCONI, 2011b, 2012). O questionário consiste em uma técnica de observação direta extensiva, constituído por perguntas que são respondidas por escrito e sem a presença do pesquisador (LAKATOS E MARCONI, 2011a). O questionário desenvolvido se encontra no anexo A. Assim, após a realização das entrevistas e aplicação dos questionários, foi possível obter uma lista de critérios relevantes à escolha de um modelo.

Embora a lista de critérios obtida representasse a opinião de especialistas, esta poderia ter sido influenciada por tendências/preferências dos entrevistados por

um determinado modelo. Desta forma, para obter um consenso confiável de opiniões do grupo de especialistas, foi aplicada a técnica Delphi, que se propõe a obter a opinião individual e anônima de especialistas sobre o ponto de vista de outros especialistas (ABNT, 2012).

Uma vez definidos os critérios que fariam parte da pesquisa, – escolhidos por consenso pelos especialistas – esses foram submetidos a uma medida de opinião (documentação direta) por um conjunto de seis servidores da Presidência da instituição, cuja atuação na organização guardava relação com o tema estudado. Participaram da avaliação servidores de áreas como: coordenação de qualidade, coordenação de gestão de tecnologia da informação, além de assessores da vice-presidência de gestão e desenvolvimento institucional. Todas as áreas representadas na pesquisa fazem parte da Diretoria Executiva da instituição, uma instância corporativa que tem por objetivo promover a inovação na gestão e fortalecer o desenvolvimento institucional (Fiocruz, 2014).

Sabendo que as opiniões são baseadas em critérios tangíveis e intangíveis, arbitrariamente escolhidos por quem toma a decisão (SAATY, 2009), foi empregada a técnica de decisão multicritério *AHP - Analytic Hierarchy Process*, que segundo Vargas (2009) é um dos principais modelos matemáticos para apoio à teoria de decisão disponível no mercado.

Para a aplicação da técnica, os critérios selecionados foram organizados em grupos hierárquicos e submetidos à avaliação, com o apoio de um formulário (anexo B). Segundo Lakatos e Marconi (2011a), o formulário é uma técnica de observação direta extensiva e consiste em um roteiro de perguntas que são enunciadas e preenchidas pelo pesquisador a partir das respostas do pesquisado. Foi realizado um pré-teste para validação do formulário e do processo de coleta de dados, onde os entrevistados manifestaram suas percepções através de um questionário aplicado ao fim da simulação.

Desta forma, foi possível alinhar a opinião e expectativas dos gestores da instituição a partir de critérios definidos por especialistas e selecionar um modelo para o desenvolvimento de ferramentas de coleta de dados e avaliação de maturidade a partir da pontuação obtida através da técnica de decisão multicritério AHP, que será apresentada em detalhes a seguir.

3.2.1. Técnica de Decisão Multicritério AHP (Analytic Hierarchy Process)

As organizações estão inseridas em ambientes dinâmicos, assim, conhecer os critérios adequados para a tomada de decisão e fazer escolhas certas, torna-se uma tarefa vital para a sobrevivência dessas organizações. Segundo Saaty (2009), a tomada de decisão é, em sua totalidade, um processo mental cognitivo resultante da seleção do curso mais adequado de ação, baseado em critérios tangíveis e intangíveis arbitrariamente escolhidos por quem toma a decisão.

Para Vargas (2009), um dos principais desafios das organizações está na sua capacidade de fazer escolhas certas e consistentes, de modo alinhado com seu direcionamento estratégico. Bhushan & Rai (2004) ressaltam que os problemas onde as percepções humanas e julgamentos estão envolvidos, cujas soluções tem repercussões de longo prazo, exigem uma abordagem racional para a solução.

O *Analytic Hierarchy Process* – AHP é uma técnica multicritério para a tomada de decisão em ambientes complexos em que diversas variáveis ou critérios são considerados para a priorização e seleção de alternativas (VARGAS, 2009). Segundo Triantaphyllou (1995), a técnica AHP é uma ferramenta de suporte a decisão que pode ser usada para a solução de problemas complexos. A técnica foi desenvolvida por Thomas L. Saaty na década de 1970 e desde então tem sido exaustivamente utilizada para a tomada de decisão em situações que exigem percepções e julgamentos humanos.

A técnica consiste em decompor um problema em uma hierarquia de critérios, permitindo ser analisado e comparado mais facilmente de forma independente. Uma vez definida a hierarquia lógica, os tomadores de decisão podem avaliar as alternativas de forma sistemática através da comparação de pares de critérios. A técnica AHP permite transformar comparações, por vezes empíricas, em valores numéricos que podem ser processados e avaliados.

Ao final, cada critério receberá um peso que é utilizado para a comparação dos elementos de acordo com a hierarquia definida. “A capacidade de conversão de dados empíricos em modelos matemáticos é o principal diferencial da AHP com relação a outras técnicas comparativas” (VARGAS, 2009).

A técnica AHP utiliza a escala proposta por Thomas L. Saaty, denominada escala Saaty para comparar a importância entre elementos. Embora a comparação possa ser realizada de diferentes formas, a escala Saaty é a mais amplamente utilizada com a técnica AHP (VARGAS, 2009).

Tabela 4: Escala Saaty para medição em comparação de pares (Saaty, 2006)

Escala de Saaty de medição em comparação emparelhada		
Intensidade da importância {1}	**Definição {2}**	**Explanação {3}**
1	Igual importância	Duas atividades contribuem igualmente para o objetivo
3	Moderada importância	Experiência e julgamento levemente a favor de um em relação ao outro
5	Forte importância	Experiência e julgamento fortemente a favor de um em relação ao outro
7	Muito forte importância	Uma atividade é fortemente favorecida e seu domínio é demonstrado na prática
9	Absoluta importância	A importância de um em relação ao outro ratifica sua superioridade
2, 4, 6, 8	Valores intermediários	Usado para representar o ajuste entre as prioridades listadas acima
Reciprocidade de números diferentes de zero		Se uma atividade *i* tem um número diferente de zero associado, quando comparado à atividade *j*, então *j* tem o valor recíproco quando comparado a *i*.

Conforme pode ser observado na tabela 4, a escala trabalha com valores que variam entre 1 e 9, e seus recíprocos, que determinam a importância relativa entre dois elementos (SAATY, 2006). Embora as descrições estejam associadas aos valores impares, é possível utilizar os valores pares para representar uma opinião intermediária.

Para ilustrar a aplicação da técnica AHP, tomemos como exemplo a avaliação das preferências de um entrevistado em relação ao critério 'dirigibilidade' entre cinco modelos de automóveis, conforme figura abaixo:

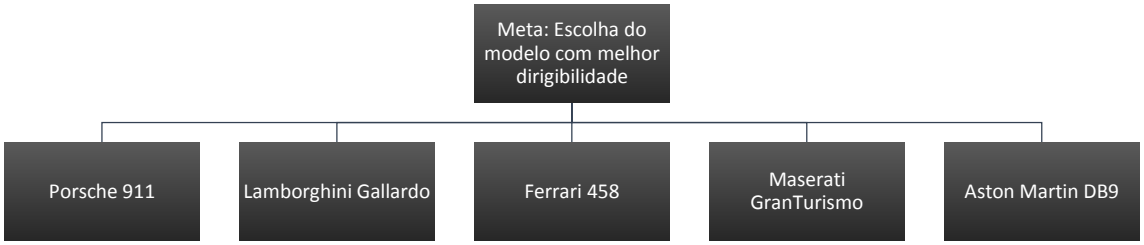


Figura 14: Exemplo de um grupo hierárquico de critérios

Uma vez definida a estrutura hierárquica de critérios para avaliação – neste exemplo representado por cinco modelos de automóveis (Porsche 911, Lamborghini Gallardo, Ferrai 458, Maserati GranTurismo e Aston Martin DB9) – é possível definir uma matriz comparativa, conforme a figura abaixo:

Tabela 5: Exemplo de matriz comparativa de critérios

	Porsche 911	Lamborghini Gallardo	Ferrai 458	Maserati GranTurismo	Aston Martin DB9
Porsche 911					
Lamborghini Gallardo					
Ferrai 458					
Maserati GranTurismo					
Aston Martin DB9					
Total					

A partir dessa matriz, os critérios são tomados em pares para que cada participante opine sobre a importância de um critério em detrimento a outro. Tomemos como exemplo a matriz preenchida abaixo, cujos valores representam os graus de importância definidos na escala Saaty.

Tabela 6: Exemplo de matriz comparativa preenchida segundo escala Saaty

	Porsche 911	Lamborghini Gallardo	Ferrai 458	Maserati GranTurismo	Aston Martin DB9
Porsche 911	1	1/4	1/2	1/3	5
Lamborghini Gallardo	4	1	4	1	5
Ferrai 458	2	1/4	1	1/3	4
Maserati GranTurismo	3	1	3	1	3
Aston Martin DB9	1/5	1/5	1/4	1/3	1
Total	**10,20**	**2,70**	**8,75**	**3,00**	**18,00**

No exemplo acima a diagonal principal da matriz está preenchida com o valor 1, pois se refere a comparação entre os mesmos elementos (Porsche 911 x

Porsche 911, Lamborghini Gallardo x Lamborghini Gallardo, Ferrai 458 x Ferrai 458, etc.), ou seja, apresentando o mesmo grau de importância.

Ainda no exemplo, o valor da comparação entre 'Porsche 911' e 'Aston Martin DB9' foi definido como 5, indicando uma preferência forte (valor 5) pelo modelo 'Porsche 911', sendo o seu recíproco (Aston Martin DB9) $^1/_5$. Outro exemplo é a comparação entre 'Maserati GranTurismo' e 'Ferrai 458', onde o valor 3 indica uma preferência moderada pelo modelo 'Maserati GranTurismo' e o seu recíproco (Ferrai 458) possui o valor $^1/_3$. Para calcular e interpretar os pesos relativos de cada modelo, faz-se necessário normalizar a matriz anterior através da divisão de cada valor da matriz pelo total calculado pelas colunas (total de cada modelo). Sendo assim, temos:

Tabela 7: Exemplo de matriz comparativa com valores normalizados

	Porsche 911	Lamborghini Gallardo	Ferrai 458	Maserati GranTurismo	Aston Martin DB9	Média
Porsche 911	0,10	0,09	0,06	0,11	0,28	0,13
Lamborghini Gallardo	0,39	0,37	0,46	0,33	0,28	0,37
Ferrai 458	0,20	0,09	0,11	0,11	0,22	0,15
Maserati GranTurismo	0,29	0,37	0,34	0,33	0,17	0,30
Aston Martin DB9	0,02	0,07	0,03	0,11	0,06	0,06
Total	**1,00**	**1,00**	**1,00**	**1,00**	**1,00**	**1,00**

A próxima etapa é a verificação da consistência dos dados em relação às opiniões emitidas. Chamemos o modelo 'Porsche 911' de critério A, 'Lamborghini Gallardo' de critério B e 'Ferrai 458' de critério C. Caso um entrevistado defina que o critério A é mais importante que o critério B e que o critério B é mais importante que o critério C, seria inconsistente afirmar em algum momento, por exemplo, que o critério C é mais importante que o critério A, pois se $A > B > C$, então não podemos afirmar que $A < C$.

Para avaliação da consistência, Saaty (2005) define um índice de consistência (CI, do inglês *consistency index*) dado pela equação:

$$CI = \frac{\lambda_{Max} - n}{n-1}$$

Onde, λ_{Max} é o resultado da média dos valores obtidos pela ponderação dos critérios (tabela 6) pela média dos critérios (tabela 7), dividido pela média dos critérios (tabela 7). A variável n representa o número de critérios sendo avaliados.

Sendo assim temos:

$$CI = \frac{5{,}4354 - 5}{4} = 0{,}11$$

Para saber se o valor encontrando no índice de consistência é adequado, Saaty (2005) propôs uma taxa de consistência (CR, do inglês *consistency rate*), determinado pela razão entre o CI e o índice de consistência aleatório (RI, do inglês *random index*).

$$CR = \frac{CI}{RI}$$

O RI é uma constante obtida de acordo com o valor de n, podendo assumir os seguintes valores:

Tabela 8: Tabela de índices de consistência aleatória (Saaty, 2005)

n	1	2	3	4	5	6	7	8	9	10
RI	0	0	0,58	0,90	1,12	1,24	1,32	1,41	1,45	1,49

Desta forma, temos:

$$CR = \frac{0{,}11}{1{,}12} = 0{,}09 = 9\%$$

Para que uma matriz seja considerada consistente, o valor obtido em CR deve ser menor que 10%. No exemplo acima, foi obtido um valor de 0,09 (9%), portanto a matriz estaria consistente. Caso o CR apresentado fosse maior que 10%, seria necessário revisar as respostas dadas em busca de incoerências na avaliação.

3.3. Desenvolvimento, especificação e aplicação do instrumento de avaliação

O terceiro objetivo consiste na proposição de um instrumento de coleta de dados e avaliação de maturidade em gestão de riscos de TI, a especificação dos requisitos funcionais para a construção de uma ferramenta automatizada para apoio ao processo de avaliação de maturidade e a simulação da aplicação do instrumento proposto em uma unidade de TI da organização para sua validação.

Para a proposição do instrumento de avaliação foi realizada uma pesquisa documental mais aprofundada no modelo de maturidade selecionado, permitindo conhecer o método de avaliação e os elementos necessários para a definição do instrumento. Foi utilizada a ferramenta Excel para a prototipação de um instrumento para o registro dos dados coletados e automatização do processo de avaliação de maturidade em gestão de riscos de TI.

Uma vez definido o instrumento de avaliação, foram especificados os requisitos funcionais para a definição de uma ferramenta automatizada para apoio ao processo de avaliação de maturidade em gestão de riscos de TI. Essa especificação foi realizada segundo a Metodologia de Desenvolvimento de Sistemas da Fiocruz, desenvolvida através de uma parceria da Fiocruz com a COPPE UFRJ e que se encontra em fase de homologação.

A Metodologia de Desenvolvimento de Sistemas utilizada está alinhada à norma ISO/IEC/IEEE 29148:2011, que dispõe sobre os processos e produtos relacionados à engenharia de requisitos, e que substitui os padrões IEEE 830-1998 (Prática recomendada para especificações de requisitos de software), IEEE 1233-1998 (Processo do ciclo de vida da engenharia de requisitos) IEEE 1362-1998 (Definição do sistema) e se alinha as normas ISO/IEC 12207 (Processo de ciclo de vida de software) e ISO/IEC 15288 (Processos de ciclo de vida de sistemas).

Por fim, foi realizada uma avaliação de maturidade para validação do instrumento proposto e identificação do nível de maturidade em gestão de riscos de TI. Para isso, foi realizada uma pesquisa de campo para levantamento de dados junto a Coordenação de Gestão de Tecnologia da Informação, através do método de observação direta extensiva, tendo como técnica empregada o formulário (desenvolvido em Excel) para registro dos dados coletados e avaliação automatizada do nível de maturidade.

Capítulo 4

Resultados e Discussão

4.1. Análise Comparativa dos Modelos de Maturidade

Para a análise comparativa foi identificado um conjunto de modelos de maturidade candidatos ao estudo proposto, encontrados em *frameworks* de mercado, propostas acadêmicas e norma de referência. São eles: CMMI 1.3, COBIT 4.1, COBIT 5, ERM, FVSAH, ISO/IEC 15504 e RMM. No entanto, ao longo do trabalho foram descartados dois modelos: ERM e COBIT 5.

O ERM, desenvolvido pelo COSO, não deixava claro em sua documentação a proposta de um modelo de maturidade. A única fonte encontrada como referência no uso de um modelo de maturidade em gestão de riscos com o *framework* COSO foi a empresa Protiviti. Após uma interação junto a entidade mantenedora do modelo, foi informado não existir de forma nativa um modelo de maturidade no ERM, embora a entidade reconheça que algumas organizações privadas estejam empenhadas no estudo/desenvolvimento de modelos de maturidade baseados em seu framework. Assim, apesar de apresentar um modelo sólido para gestão de riscos, o modelo ERM não será utilizado neste trabalho, por não fornecer um modelo da maturidade próprio, desenvolvido e publicado.

O COBIT 5, desenvolvido pelo ISACA, não foi contemplado no estudo pois um importante guia que compõem o *framework*, "COBIT 5 *for Risk*" – com orientações sobre o gerenciamento de riscos – ainda se encontrava em desenvolvimento, restringindo o material disponível para a pesquisa. Ainda durante a pesquisa foi identificada uma alteração no modelo COBIT 4.1, que originalmente se baseava no modelo CMM e passou a se basear na família ISO/IEC 15504, assim como o COBIT 5.

Desta forma, os modelos efetivamente utilizados na pesquisa foram: CMMI 1.3, COBIT 4.1, FVSAH, ISO/IEC 15504 e RMM. Embora apenas um dos *frameworks* tenha sido desenhado especificamente para a avaliação de maturidade em gestão de riscos, os demais foram escolhidos por oferecer uma estrutura para avaliação de maturidade e por seus conteúdos, em algum grau, referenciarem a gestão de riscos, permitindo assim um recorte do tema.

4.1.1. Capability Maturity Model Integration – CMMI

A primeira versão do *Capability Maturity Model Integration* – CMMI foi lançada no ano 2000 pelo *Software Engineering Institute* – SEI – um centro de pesquisa e desenvolvimento do governo dos Estados Unidos da América – sendo patrocinado pelo Departamento de Defesa – DoD. Em 2010 foi lançada a mais recente família CMMI, correspondente à versão 1.3. Seu domínio de aplicação é a melhoria dos processos para a prestação de serviços e sua criação está baseada em três documentos de referência: *Capability Maturity Model for Software* (CMM-SW/SEI), *Systems Engineering Capability Model* (SECM/EIA) e *Systems Engineering Capability Assessment Model* (SECAM/INCOSE).

O CMMI permite dois tipos de representação: contínua e por estágios. Na representação contínua a organização pode focar em um processo isolado que necessita ser melhorado, permitindo visibilidade crescente da capacidade alcançada em cada área de processo. Já a representação por estágios aborda a melhoria do processo enfocando um estágio por vez, de forma a assegurar que foi estabelecida a infraestrutura adequada de processos que servirá de base para o próximo estágio.

O CMMI, quando utilizado na abordagem por estágios, apresenta cinco níveis de maturidade:

Nível 1: Inicial

Nível 2: Gerenciado

Nível 3: Definido

Nível 4: Gerenciado quantitativamente

Nível 5: Em otimização

Para a progressão entre os níveis, devem ser observadas as dependências entre as práticas genéricas e as áreas de processo. Assim, este modelo impõe pré-requisitos em função das atividades, produtos de trabalho e serviços do processo que devem ser observados ao se executar uma avaliação.

Embora os instrumentos de avaliação não sejam oferecidos pelo modelo, este diz que os instrumentos podem assumir diversas formas, tais como questionários, inquéritos, pacotes de orientação do site, mapeamentos das boas práticas do modelo de referência, etc., mas que devem ser definidas e implementadas pela organização (SEI, 2011).

Em relação à rastreabilidade, o modelo prevê que os objetivos de mediação sejam identificados e registrados, de forma a permitir sua comparação em caso de mudanças nos objetivos ou ainda sua evolução.

Outra característica relevante é a possibilidade de comparação dos resultados da avaliação de maturidade de uma organização com outras organizações similares. O CMMI permite essa comparação, mas não prevê de forma nativa os mecanismos para que seja feita. Para isso, indica um método externo de avaliação denominado SCAMPI. O documento *Standard CMMI Appraisal Method for Process Improvement: Method Definition Document* – SCAMPI define regras para assegurar a objetividade na classificação das avaliações.

Para que seja possível o *benchmarking* com outras organizações, as avaliações devem assegurar que as classificações sejam comparáveis, pois, alcançar um nível de maturidade específico ou satisfazer uma área de processo deve ter o mesmo significado para diferentes organizações avaliadas (SEI, 2010). Existem três tipos de avaliação: Classe A, Classe B e Classe C, onde as avaliações do tipo B e C são menos formais e a avaliação de Classe A considerada a mais rigorosa, sendo o único tipo de avaliação válida para o *benchmarking*.

Em relação à customização do modelo, o SEI (2010) diz que o CMMI permite a customização desde que sejam contemplados os elementos essenciais de processos efetivos de uma ou mais disciplinas e que sejam descritos um caminho de melhoria evolutiva desde processos imaturos, *ad hoc*, até processos maduros, disciplinados, com qualidade e eficácia melhoradas. O SEI diz ainda que, independentemente do tipo de organização, deve-se utilizar discernimento ao aplicar as melhores práticas, levando em consideração a situação, as necessidades e os objetivos estratégicos da organização.

Embora as áreas de processo descrevam as características de uma organização comprometida com melhoria de processo, deve-se interpretar as áreas de processo à luz de conhecimento aprofundado do CMMI, da organização, do ambiente de negócio e das circunstâncias específicas envolvidas.

Por fim, em relação aos custos para implementação do CMMI, o *CMMI Institute* (2013) disponibiliza toda a documentação sem custos, inclusive o método

SCAMPI. Já em relação ao treinamento, existe um custo de aproximadamente R$ 7.043,00, referente ao curso introdutório (CMMI Institute, 2013).

4.1.2. Control Objectives for Information and related Technology – COBIT 4.1

O COBIT 4.1 foi desenvolvido em 2007 pelo *IT Governance Institute* - IGTI e atualmente é mantido pelo *Information Systems Audit and Control Association* – ISACA, ainda com a ajuda do ITGI. Seu domínio de aplicação é o Controle e Gerenciamento de TI, focado no que é necessário para que as organizações alcancem um adequado controle e gerenciamento de TI.

Em sua elaboração foram considerados outros documentos de referência, tais como: ITIL, ISO 17799, PMBOK, PRINCE2, VAL IT, ISO/IEC 15504-1, ISO/IEC 15504-2 (ITGI, 2007). O modelo de maturidade do COBIT 4.1, originalmente, se baseava no CMM, porém, em seu programa de avaliação chamado COBIT *Assessment Programme*, passou a adotar como base a norma ISO/IEC 15504. A escala de maturidade original do COBIT 4. 1 continha seis níveis de maturidade (ITGI, 2007):

Nível 0: Inexistente;

Nível 1: Inicial;

Nível 2: Repetível;

Nível 3: Definido;

Nível 4: Gerenciado e mensurado;

Nível 5: Otimizado;

Em relação ao COBIT 4.1 baseado no novo programa de avaliação, a escala manteve a mesma quantidade de níveis, porém com novas descrições (ISACA, 2011a, 2011b):

Nível 0: Incompleto;

Nível 1: Executado;

Nível 2: Gerenciado;

Nível 3: Estabelecido;

Nível 4: Previsível;

Nível 5: Em otimização

Outra mudança significativa foi o fato de o COBIT 4.1 original não impor dependência entre os níveis de maturidade, enquanto o COBIT 4.1 baseado na família ISO/IEC 15504 exigir pré-requisitos antes de se alcançar um novo nível de maturidade. Ou seja, faz-se necessário ter cumprido todas as condições do nível.

Em relação aos instrumentos de avaliação, o modelo se mostra bastante flexível, onde as avaliações podem ser executadas com base nas descrições do nível de maturidade como um todo ou com um maior rigor a partir de afirmações individuais dessas descrições. O modelo oferece ainda *templates* que podem ser utilizados ou adaptado pelas organizações para aplicação.

O novo modelo define os requisitos para a documentação e controle de produtos de trabalho, incluindo a identificação as dependências, aprovações e rastreabilidade dos requisitos. O modelo oferece a possibilidade de comparação com outras organizações. Segundo o ISACA (2011a), os valores obtidos nas avaliações incluem resultados confiáveis da empresa sobre os riscos, benefícios e implicações de recursos decorrentes do desempenho e da capacidade dos seus processos de TI, fornecendo uma base sólida para o *benchmarking* e melhoria, priorização e planejamento.

É possível customizar o modelo para aplicação em uma organização específica, pois os objetivos apresentados são genéricos e devem ser utilizados como um guia (IGTI, 2007). Em relação aos custos, tanto o material de referência quanto a capacitação são pagas. O material básico[1] necessário para a implementação tem um custo estimado de R$ 469,56. A capacitação no próprio ISACA tem um valor estimado de R$ 1.291,29.

4.1.3. Formação de Valor em Sistemas de Atividades Humanas – FVSAH

O modelo de maturidade FVSAH (Formação de Valor em Sistemas de Atividades Humanas) foi proposto em 2012 pelo professor Dr. João Mello da Silva, do Departamento de Engenharia de Produção (EPR) da Universidade de Brasília (UnB).

O modelo proposto é genérico, permitindo sua aplicação em qualquer escopo. Sua escala de maturidade possui cinco níveis com as seguintes descrições:

[1] Foram considerados os seguintes documentos: COBIT 4.1; COBIT Process Assessment Model (PAM): Using COBIT; Assessor Guide: Using COBIT; e COBIT Self-Assessment Guide: Using COBIT.

Nível 1: Funcionamento;

Nível 2: Especialização;

Nível 3: Crescimento;

Nível 4: Convergência;

Nível 5: Referência;

Para a progressão a um nível de maturidade mais alto, faz-se necessário completar os requisitos do nível atual. O modelo não prevê mecanismos de rastreabilidade das evidências utilizadas para o posicionamento em um determinado nível, mas contempla o *benchmarking* com organizações similares.

Por ser um modelo genérico é necessária sua customização em relação ao negócio da organização antes da sua aplicação, o que torna o modelo flexível. O material é disponibilizado gratuitamente, mas em contra partida não existe um programa de capacitação.

4.1.4. ISO/IEC 15504

A família de normas brasileiras 15504 foi publicada 2008 pela Associação Brasileira de Normas Técnicas – ABNT, sendo uma tradução das normas internacionais da família 15504 desenvolvidas pela *International Organization for Standardization* – ISO.

Trata-se de um modelo genérico que aborda a avaliação de processo, onde o modelo de referência é definido externamente. Assim, para a aplicação do modelo de avaliação de maturidade do processo de gestão de riscos é necessário utilizar um modelo de referência externo, tal como a norma ISO 31000.

Sua construção tem por base um conjunto de outros documentos de referência, tais como: ISO 9000, ISO/IEC 2382-1, ISO/IEC 2382-20, ISO/IEC 12207 e ISO/IEC 15288. Sua escala possui 6 níveis de maturidade, definidos como:

Nível 0: Incompleto;

Nível 1: Executado;

Nível 2: Gerenciado;

Nível 3: Estabelecido;

Nível 4: Previsível;

Nível 5: Em otimização

O modelo proposto exige uma dependência entre os níveis de maturidade, onde para se alcançar um determinado nível é necessário que todos os processos atribuídos aquele nível e aos níveis anteriores tenham sido alcançados. Em relação aos instrumentos de avaliação, o modelo não os fornece, mas apresenta considerações para a sua seleção.

O modelo prevê de forma explícita a necessidade de manter a rastreabilidade entre a pontuação de um atributo e a evidência objetiva utilizada para se determinar uma pontuação. A norma traz ainda como benefícios a capacidade da avaliação de processos prover uma comparação objetiva entre organizações (*benchmarking*) e a possibilidade de customização para aplicação em um domínio específico ou organização.

Em relação aos custos, o material de referência (ABNT NBR ISO/IEC 15504-1:2008, ABNT NBR ISO/IEC 15504-2:2008, ABNT NBR ISO/IEC 15504-3:2008, ABNT NBR ISO/IEC 15504-4:2008, ABNT ISO/IEC TR 15504-6:2009, ABNT ISO/IEC TR 15504-7:2009) tem um custo de R$ 555,00 e a capacitação R$ 1.080,00.

4.1.5. Risk Maturity Model – RMM

O *Risk Maturity Model* – RMM foi desenvolvido em 1997 pelo Dr. David A. Hillson e propõe um modelo de maturidade de gerenciamento de riscos com quatro níveis de maturidade independentes, descritos da seguinte forma:

Nível 1: Ingênuo;

Nível 2: Principiante;

Nível 3: Normalizado;

Nível 4: Natural;

Mesmo não sendo oferecido um instrumento de avaliação, o autor sugere um questionário de avaliação (Hillson, 2002). O modelo não indica ou recomenda a preservação dos elementos que evidenciam o alcance de um determinado nível, mas prevê a comparação com organizações similares. Embora não esteja explicitamente previsto, o modelo pode ser adaptado, como fez Hopkinson (2011) adaptando o RMM para aplicação na gestão de riscos de projetos. O modelo está disponível na forma de artigos, mas não há capacitação no modelo.

4.1.6. Matriz comparativa dos modelos de maturidade em gestão de riscos

Com base nas informações descritas em de cada um dos modelos apresentados anteriormente, foi construída uma matriz resumida, que permite comparar de forma sintética as principais características dos modelos. A matriz apresenta a comparação entre treze características: quantidade de níveis, descrição das escalas de maturidade, dependência entre níveis, domínio do modelo de referência, instrumentos de avaliação, entidade mantenedora, alinhamento com outros instrumentos, tempo de mercado, rastreabilidade, *benchmarking*, customização, custo com capacitação e custo do material.

Embora os modelos estudados tenham sido organizados por diferentes entidades e para diferentes finalidades, podemos observar que algumas características são comuns entre determinados modelos. Por exemplo: quantidade de níveis de maturidade (existem dois modelos com cinco níveis e dois modelos com seis níveis), dependência entre níveis (apenas um dos modelos não exige a dependência de níveis inferiores, para todos os outros é exigido), instrumentos de avaliação (apenas um modelo oferece um instrumento para apoio ao processo de avaliação, os demais não), rastreabilidade (quatro dos cinco modelos tratam da rastreabilidade das avalições), *benchmarking* e customização.

A seguir é apresentada a tabela comparativa resumida com as principais características dos modelos de maturidade estudados.

Tabela 9: Tabela comparativa resumida dos modelos de maturidade em gestão de riscos

Características	CMMI 1.3	COBIT 4.1	FVSAH	ISO/IEC 15504	RMM
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
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 (Silva)	ABNT/ISO	Acadêmico (Hillson)
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
Rastreabilidade	Sim	Sim	Não	Sim	Não
Benchmarking	Dependente de método externo	Nativo	Nativo	Nativo	Nativo
Customização	Sim	Sim	Sim	Sim	Não
Custo com capacitação[2]	7.043,40	1.291,29	-	1.080,00	-
Custo do material[3]	-	469,56	-	555,00	-

[2] Valores aproximados, referentes aos cursos introdutórios

[3] Valores aproximados, referentes a documentação básica

4.2. Seleção do Modelo de Maturidade

Como pôde ser visto na matriz comparativa, existem diversos modelos de maturidade que podem ser aplicados à gestão de riscos de TI, cujas características podem ser adequadas a uma ou outra organização. Desta forma, este capítulo se propõe a apresentar um método como forma de atingir o objetivo específico dois deste trabalho que é o de selecionar, junto aos modelos estudados, um modelo de maturidade cujos aspectos melhor atendam, em parte ou íntegra, expectativas da organização no que se refere à gestão de riscos de TI.

Para a seleção do modelo de maturidade foi necessário identificar um conjunto de critérios que pudessem ser utilizados para essa escolha. A seguir são apresentados os critérios que, na opinião dos especialistas entrevistados (vide item 3.2), deveriam ser considerados para a escolha do modelo:

- Nome dos níveis de maturidade na escala, de forma que sejam suficientemente claros (autoexplicativos);
- Possibilidade de comparação dos resultados da avaliação com instancias similares (*Benchmarking*);
- Indicação dos caminhos para a melhoria do processo de gestão de riscos;
- Possibilidade de auto avaliação, ou seja, uma avaliação realizada por membros da própria organização;
- Simplicidade do modelo, sendo de fácil assimilação e aplicação;
- Quantidade de níveis (da escala) do modelo de maturidade;
- Equivalência de esforços para a mudança de nível;
- Clareza/objetividade das boas práticas sugeridas no modelo;
- Processo de avaliação de maturidade claramente definido;
- Domínio de aplicação do modelo (aderência ao negócio);
- Tempo/prazo necessário para a implementação;
- Custo de implementação (capacitação, guias, manuais, normas, etc.);
- Instrumentos de avaliação (questionários, planilhas, etc.) oferecidos pelo modelo;
- Robustez do modelo;
- Alinhamento com documentos de referência;
- Tempo em uso no mercado;
- Disponibilidade de consultoria prática;
- Experiência de outros órgãos na adoção do modelo;
- Dependência entre níveis (necessidade ou não de cumprir pré-requisitos necessários para alcançar um determinado nível);

- Público-alvo;
- Entidade mantenedora;
- Rastreabilidade dos elementos utilizados para o alcance de um nível;
- Possibilidade de customização do modelo para aplicação em outros domínios ou ainda sua adaptação a uma organização;

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 e consequentemente, quais não deveriam ser utilizados. Desta forma, foram excluídos:

- Tempo/prazo necessário para a implementação;
- Público-alvo

Entre os modelos estudados, alguns critérios apresentavam as mesmas características e não influenciariam nos resultados. Assim, não foram selecionados para a etapa seguinte da pesquisa, uma vez que todos obteriam a mesma pontuação e aumentariam a complexidade da avaliação. São eles:

- Indicação dos caminhos para a melhoria do processo de gestão de riscos;
- Possibilidade de auto avaliação, ou seja, uma avaliação realizada por membros da própria organização;
- Processo de avaliação de maturidade claramente definido;

Dentre os critérios apresentados, alguns demandariam a implementação prática dos modelos e sua medição para que o julgamento fosse possível, sendo então descartados os seguintes critérios:

- Simplicidade do modelo, sendo de fácil assimilação e aplicação;
- Equivalência de esforços para a mudança de nível;
- Clareza/objetividade das boas práticas sugeridas no modelo;

Dois critérios também demandariam uma pesquisa de mercado para o levantamento de informações. Dado o prazo reduzido para a implementação do projeto, dois critérios foram sugeridos, mas não aplicados na pesquisa:

- Disponibilidade de consultoria prática
- Experiência de outros órgãos na adoção do modelo

Por fim, o critério 'robustez do modelo' se mostrou um tanto subjetivo, tornando sua avaliação difícil. Desta forma, outras características dos modelos de maturidade foram utilizadas para compor o critério robustez, de forma a tornar seu entendimento e avaliação mais fácil.

4.2.1. 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), que exige a definição de uma estrutura hierárquica dos critérios. A estrutura criada apresenta os treze critérios de avaliação definidos pelos especialistas através de cinco categorias: estrutura, concepção, robustez, flexibilidade e custos.

A categoria 'estrutura' apresenta os elementos que definem a forma como um modelo de maturidade está organizado. São eles: quantidade de níveis, descrição das escalas de maturidade e dependência entre níveis.

Na categoria 'concepção' são apresentadas as características sobre a forma como os modelos foram constituídos. Essa categoria é formada por: domínio do modelo de referência, instrumentos de avaliação e entidade mantenedora.

A categoria 'flexibilidade' descreve o comportamento do modelo de maturidade em relação ao mercado. As características que constituem esse agrupamento são: alinhamento com outros instrumentos e tempo de mercado.

Para categoria 'flexibilidade' são utilizados elementos que demonstram a elasticidade do modelo, ou seja, sua capacidade de se adaptar a determinadas necessidades. É constituído pelas seguintes características: rastreabilidade, *benchmarking* e customização.

Por fim, a categoria 'custos' apresenta os elementos referentes ao preço para aquisição de material e treinamento na adoção de um modelo. É formado pelas características custo com capacitação e custo do material.

A estrutura hierárquica de critérios está representada na figura abaixo:

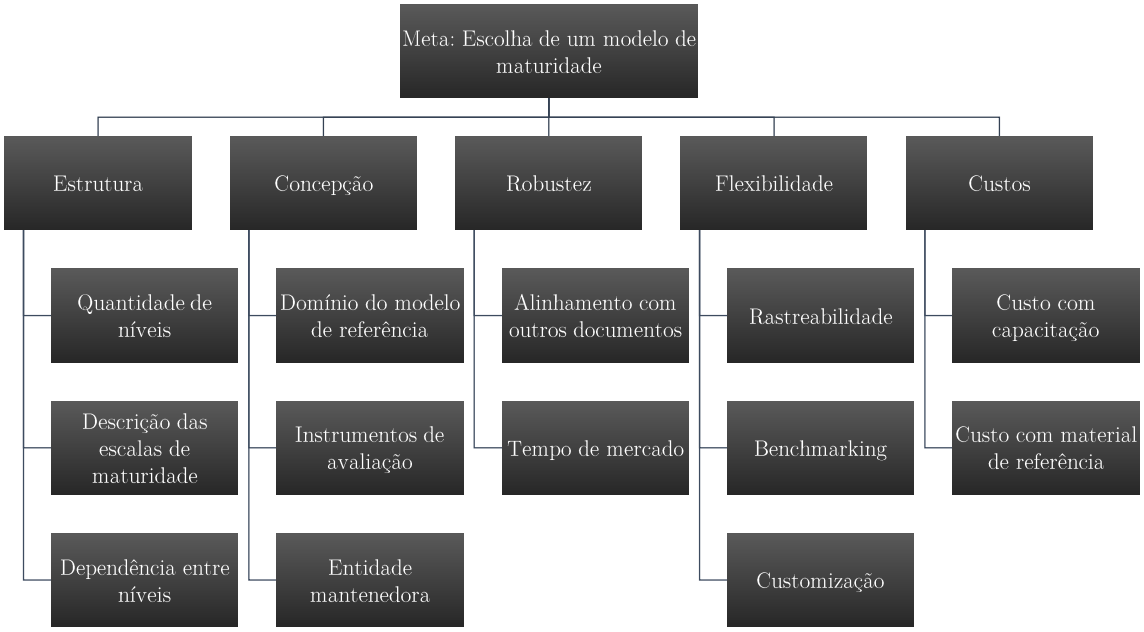


Figura 15: Estrutura hierárquica de critérios utilizados para a avaliação dos modelos de maturidade

A partir da estrutura hierárquica de critérios (figura 15) 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.

Desta forma, os três elementos geraram três comparações. No entanto, a 'quantidade de níveis' também apresenta três diferentes características: 4, 5 e 6 níveis. Desta forma, serão necessárias outras três comparações. A descrição da escala de maturidade possui quatro diferentes descrições, necessitando de seis comparações. Já o critério dependência possui apenas duas características, assim, é necessária apenas uma comparação.

Ao todo foram ouvidos seis servidores da Presidência da instituição, cuja atuação mantém relação com o escopo da pesquisa. Os entrevistados manifestaram, individualmente, sua opinião sobre cada um dos critérios definidos, através de 69 comparações.

Como a pesquisa envolveu um grande número de critérios e entrevistados, foi utilizado o software *Expert Choice* para apoio aos cálculos dos índices e também a combinação dos resultados entre os participantes (anexo D).

Antes das entrevistas com os membros da instituição foi realizado um pré-teste para validação do formulário e do processo de coleta de dados, onde foi possível observar a necessidade de alguns ajustes:

- Redesenho da escala apresentada no formulário de coleta de dados;
- Criação de um instrumento de apoio visual para a coleta de dados;
- Reordenação das questões, a fim de impor uma estrutura que facilitasse a avaliação;
- Ajustes na hierarquia de critérios e na apresentação realizada ao entrevistado (devido a uma maior incoerência encontrada nas avaliações com maior número de critérios).

4.2.2. Resultados obtidos a partir da aplicação da técnica AHP

O método utilizado para a escolha do modelo de maturidade, apesar de baseado em uma técnica bastante difundida e utilizada, trouxe uma inovação. 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 10: 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 10 apresenta os valores originais obtidos após a aplicação da técnica AHP com o apoio do software *Expert Choice*, utilizado para calcular os pesos dos critérios avaliados e combinar as respostas dos entrevistados.

Tabela 11: 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 os pesos ponderados entre os critérios de nível 1, 2 e 3 da tabela 10.

Tabela 12: 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 12 apresenta os valores da tabela 11 (pesos ponderados pela hierarquia de critérios) agrupados de acordo com os critérios principais (critérios pertencentes ao nível 1).

4.2.3. Análise dos resultados alcançados através da aplicação da técnica AHP

A seguir, cada um dos critérios do grupo principal é apresentado em forma de gráfico, descrevendo os principais resultados observados.

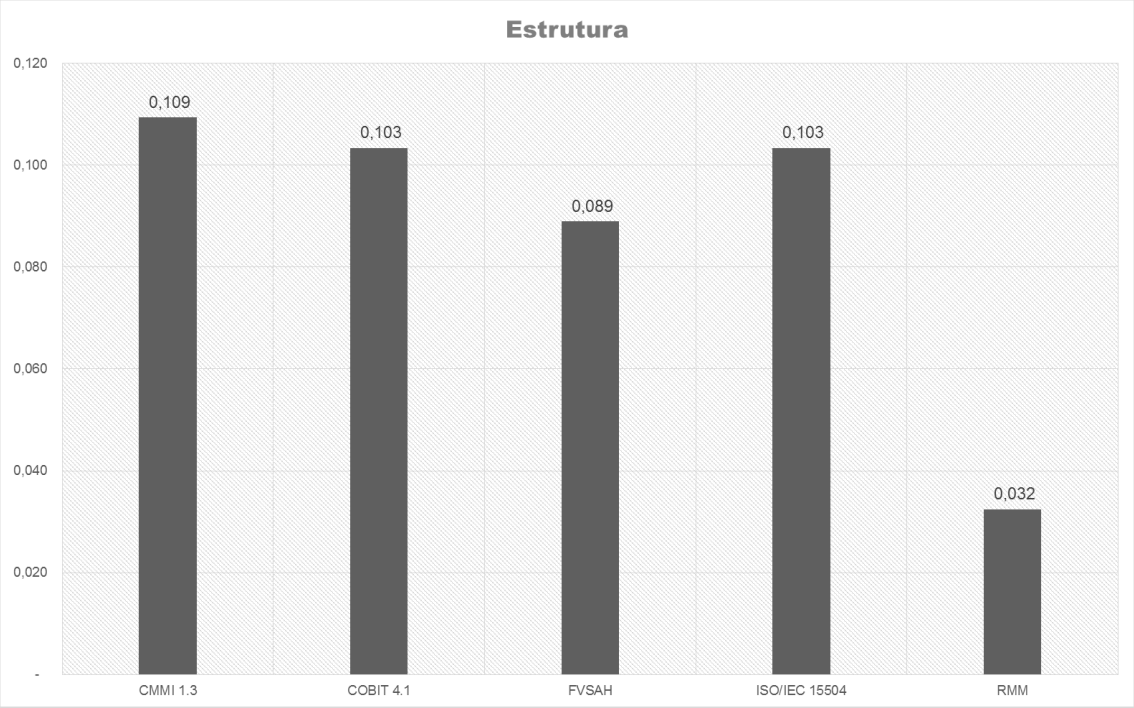


Figura 16: Pesos obtidos pelos modelos de maturidade segundo o critério de estrutura

Observa-se que no critério estrutura (referente à quantidade de níveis, descrição dos níveis e dependência entre níveis), o modelo CMMI foi o preferido pelos entrevistados, alcançando 0,109 pontos. No entanto, os modelos COBIT e ISO/IEC 15504 foram o segundo mais preferido pelos entrevistados, alcançado uma pontuação bem próxima ao primeiro com 0,103 pontos, ou seja, uma diferença de apenas 0,006 pontos.

De uma forma geral os três primeiros colocados apresentaram valores próximos, variando em torno de 5,5%. Já o modelo RMM foi o que menos agradou

aos entrevistados m relação à estrutura, alcançando 0,032 pontos (menos de 1/3 do valor alcançado pelo CMMI).

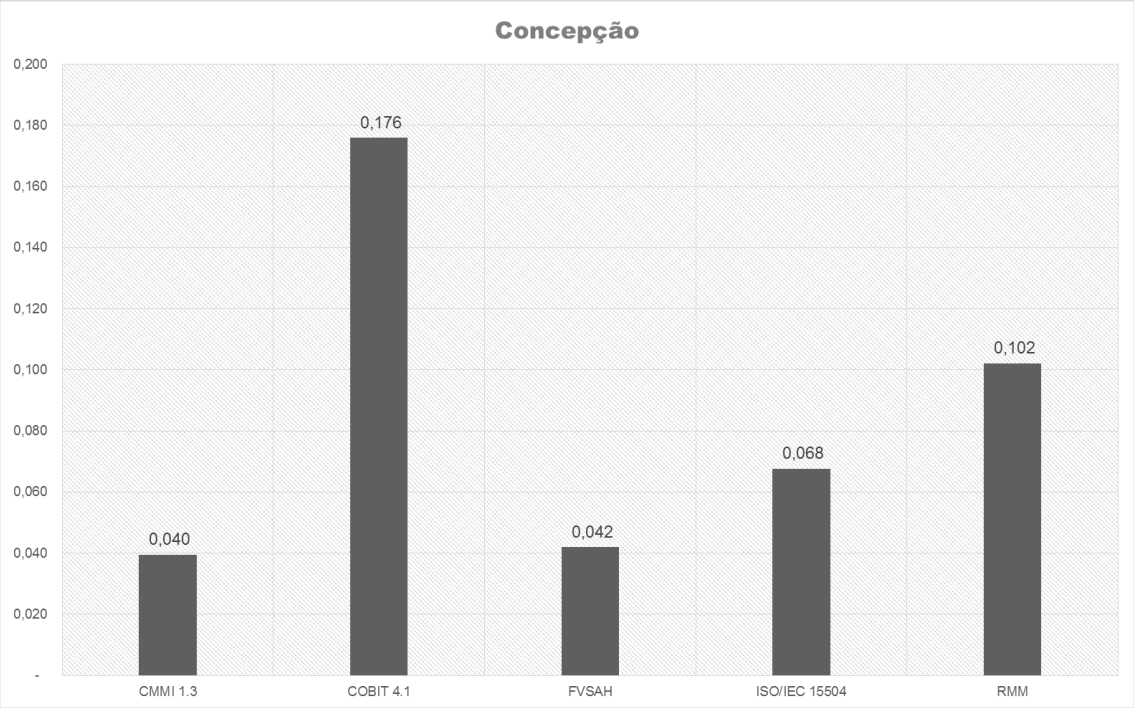


Figura 17: Pesos obtidos pelos modelos de maturidade segundo o critério de concepção

Em relação à concepção dos modelos de maturidade (referente ao domínio de referência, instrumentos de avaliação e entidade mantenedora) o COBIT foi o modelo com a melhor pontuação, alcançando 0,176 pontos. Isto representa um valor maior que a o segundo e terceiro colocados juntos.

Vale destacar que a pontuação obtida pelo modelo RMM, que na avaliação do critério estrutura ficou em último, desta vez apareceu como o segundo modelo mais preferido pelos entrevistados. Já os modelos FVSAH e CMMI ficaram na penúltima e última colocação, com pontuações parecidas, 0,042 e 0,040, respectivamente.

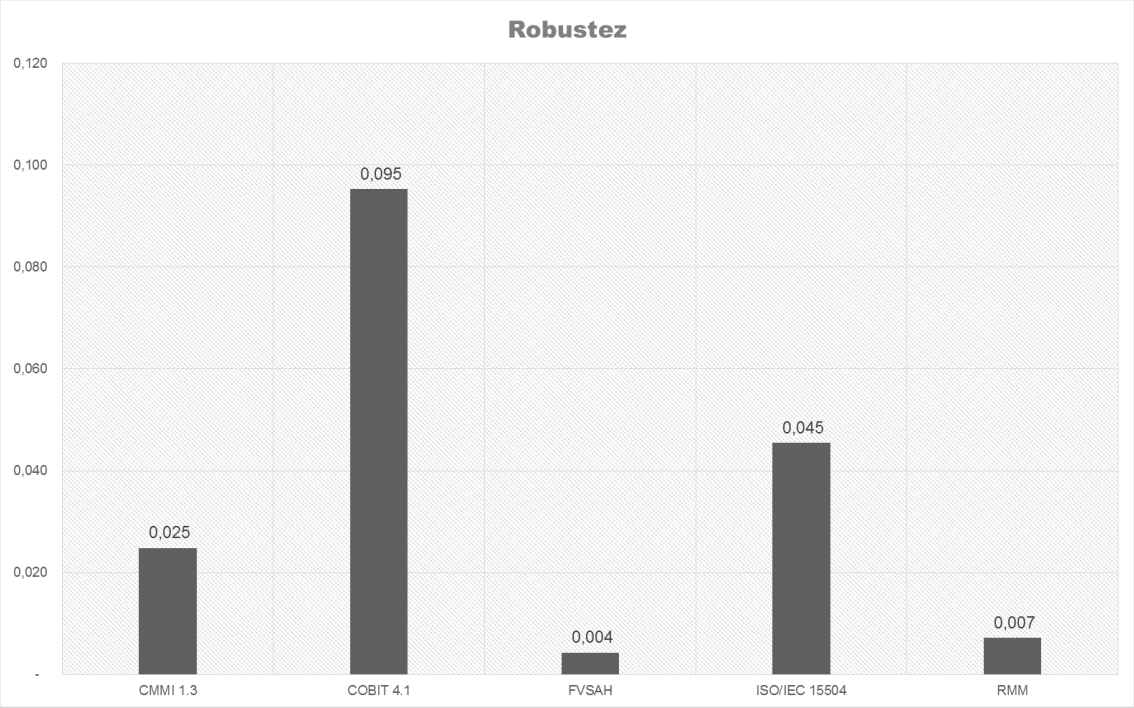


Figura 18: Pesos obtidos pelos modelos de maturidade segundo o critério de robustez

No critério robustez (referente ao alinhamento com outros documentos e tempo de mercado), mais uma vez o COBIT foi o preferido pelos entrevistados, obtendo a pontuação de 0,095. Isto representa um valor maior que a soma de todos os outros critérios (0,081 pontos).

O modelo ISO/IEC 15504 ficou em segundo com a pontuação de 0,045 (47% em relação ao primeiro) e o CMMI 0,025 (26% em relação ao primeiro). Os modelos RMM e FVSAH apresentaram pontuações muito baixas se comparado aos demais, com apenas 0,007 e 0,004 pontos, respectivamente.

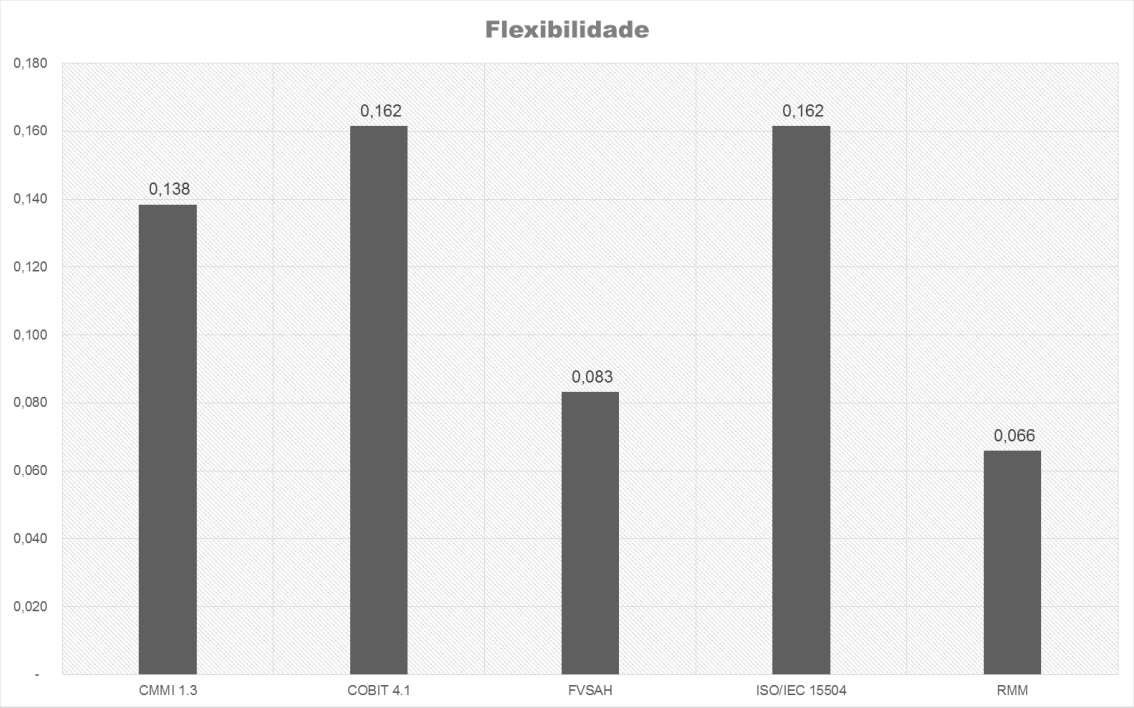


Figura 19: Pesos obtidos pelos modelos de maturidade segundo o critério de flexibilidade

Em relação à flexibilidade dos modelos de maturidade (referente aos critérios rastreabilidade, *benchmarking* e customização), os modelos COBIT e ISO/IEC 15504 empataram em primeiro lugar com 0,162 pontos, seguidos pelo CMMI com 0,138 pontos. O modelo FVSAH obteve 0,083 pontos e o RMM 0,066. O empate da pontuação entre COBIT 4.1 e ISO/IEC 15504 é esperado, tendo em vista que os modelos apresentam as mesmas características neste quesito (flexibilidade).

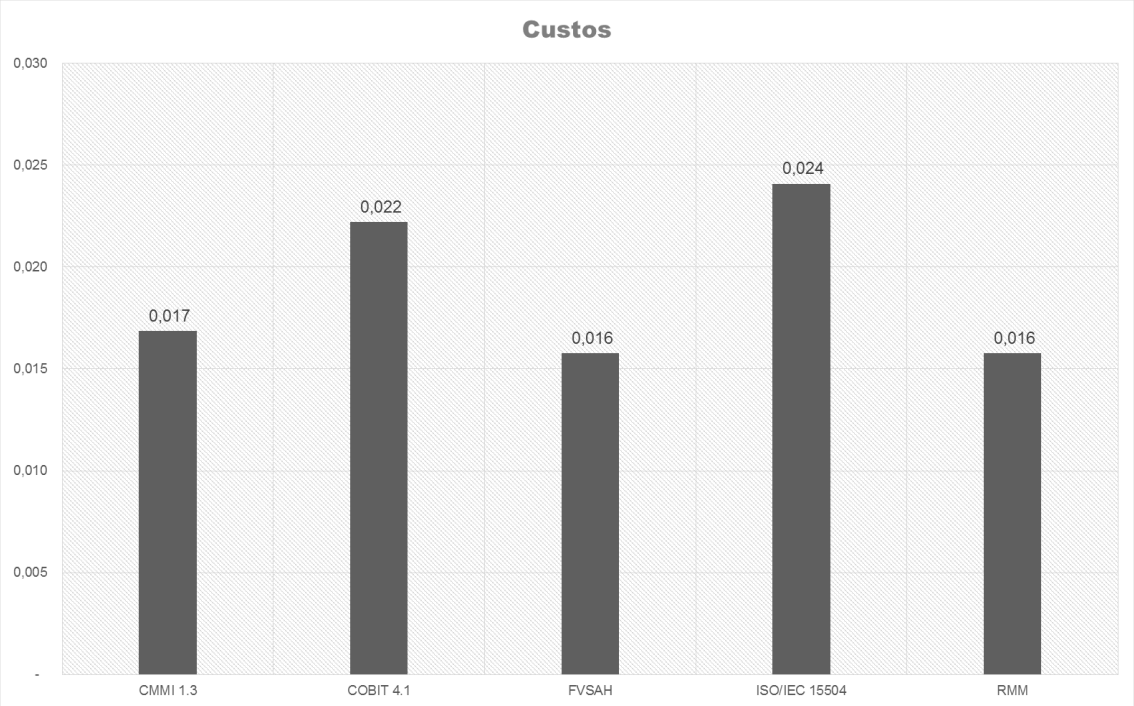


Figura 20: Pesos obtidos pelos modelos de maturidade segundo o critério de custos

Por fim, o critério custos (referente aos custos de capacitação e aquisição de material de referência) teve como modelo preferido a ISO/IEC 15504, com 0,024 pontos, seguido do COBIT com uma diferença de apenas 0,002 pontos, totalizando 0,022 pontos. Diferença menor foi observada entre o terceiro colocado, CMMI (0,017 pontos) e os modelos FVSAH e RMM, que alcançaram 0,016 pontos, ou seja, apenas 5,9%.

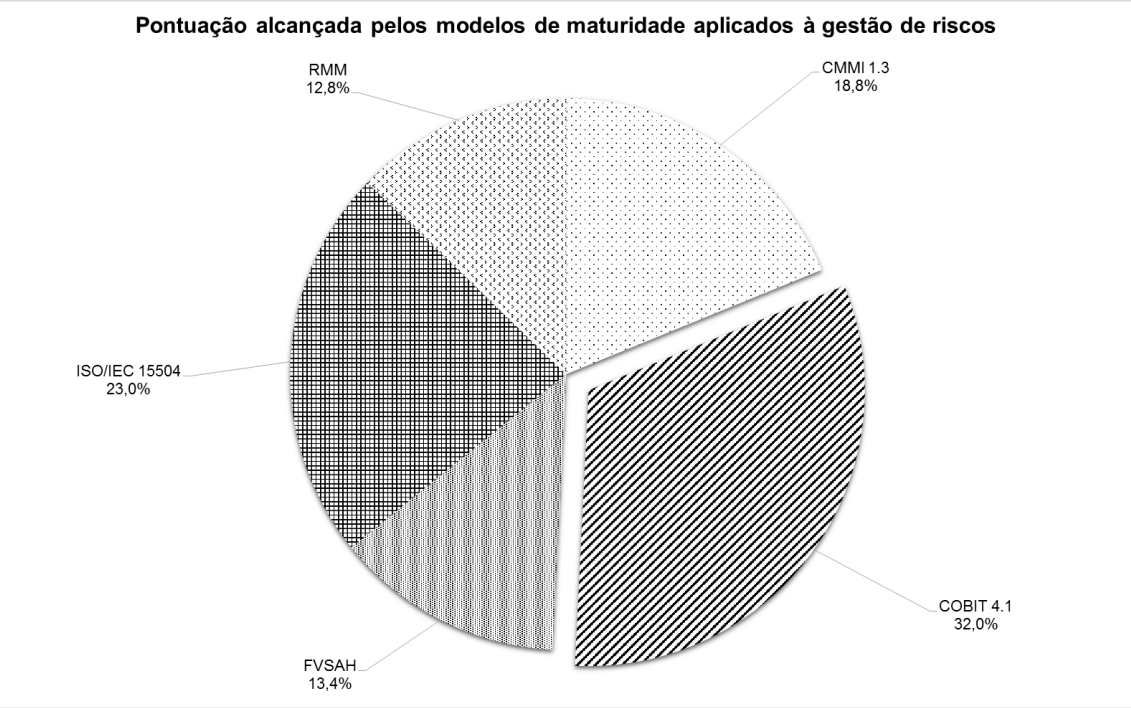
Uma vez calculado o peso ponderado dos critérios, foi possível calcular a pontuação final dos modelos, indicando assim, a preferência dos entrevistados por um modelo de acordo com suas preferências pelos critérios.

Tabela 13: 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 13 é possível verificar a pontuação final obtida por cada modelo, referente à soma dos critérios já ponderados, onde os critérios que compõem o COBIT alcançaram 0,558 pontos, seguido da ISO/IEC 15504 com 0,0402 pontos e CMMI com 0,329 pontos. Já o modelo FVSAH ficou em quarto lugar com 0,234 pontos e o RMM na quinta colocação com 0,223.

Figura 21: 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 gestores da instituição em relação aos critérios apresentados por especialistas da área, 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%).

4.3. Revisão do Modelo de Referência

O terceiro objetivo do trabalho é a proposição de um instrumento de avaliação de maturidade em gestão de riscos de TI. Na análise comparativa (veja item 4.1), o COBIT sugere um formulário padrão, não automatizado e com baixo nível de detalhamento. O Guia de Auto Avaliação do COBIT 4.1 (ISACA, 2011b) sugere ao menos dois instrumentos para apoio a auto avaliação. O primeiro instrumento é uma tabela para registro dos resultados da avaliação do processo

(anexo E). O segundo documento é um modelo para a auto avaliação (anexo F) 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. Assim, está sendo apresentado um novo instrumento de avaliação, alinhando ao 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. Para o completo entendimento do novo instrumento proposto, faz-se necessário entender o modelo de avaliação de processo original do COBIT.

4.3.1. Modelo de Avaliação de Processo do COBIT

O modelo de avaliação de processos do COBIT apresenta uma abordagem bidimensional de capacidade do processo: dimensão de processo e dimensão da capacidade. Em sua dimensão de processo, os processos são definidos e classificados em categorias. Na dimensão da capacidade, os atributos dos processos são agrupados em níveis de capacidade.

O Modelo de Referência de Processo (PRM, do inglês *Process Reference Model*) descreve cada processo com base no COBIT 4.1, definindo seu nome, propósito e resultados. Adicionalmente é definido um conjunto de Práticas Base (BP, do inglês *Base Practices*) e Produtos de Trabalho (WP, do inglês *Work Products*). As BP's proveem a definição das tarefas e atividades necessárias para a realização do propósito do processo e alcance dos resultados esperados. Cada BP está associada a um resultado do processo. Os WP's possuem um número de entradas e saídas associadas a cada um dos processos e se relacionam a um ou mais resultados.

A seguir é exibido o modelo de referência do processo para o processo PO9 (Planejar e Organizar - Avaliar e Gerenciar os Riscos de TI).

Tabela 14: Modelo de Referência do Processo PO9 – Avaliar e Gerenciar Riscos de TI (ISACA, 20011a)

ID do processo	**P09**		
Nome do Processo	**Avaliar e Gerenciar Riscos de TI**		
Propósito	Satisfazer o requisito de negócio de analisar, comunicar e gerenciar os riscos de TI e seu potencial impacto sobre os processos e objetivos de negócio.		
Resultados	**Número**	**Descrição**	
	P09-01	Uma estrutura de gestão de riscos está estabelecida e alinhada à estrutura de gestão de riscos da organização.	
	P09-02	Planos de ação para tratamento do risco são definidos e comunicados.	
Práticas Base (BP's)	**Número**	**Descrição**	**Suporta**
	P09-BP1	Determinar alinhamento da gestão de riscos (ex. avaliar o risco)	PO9-01
	P09-BP2	Entender os objetivos estratégicos relevantes do negócio	PO9-01
	P09-BP3	Entender os objetivos de processos relevantes do negócio	PO9-01
	P09-BP4	Identificar os objetivos internos de TI relacionados à gestão de riscos, e estabelecer o contexto do risco	PO9-01
	P09-BP5	Identificar os eventos associados a esses objetivos	PO9-01
	P09-BP6	Avaliar os riscos associados aos eventos	PO9-01
	P09-BP7	Avaliar respostas aos riscos	PO9-01
	P09-BP8	Priorizar e planejar atividades de controle	PO9-02
	P09-BP9	Aprovar e garantir fundos para os planos de ação de riscos	PO9-02
Produtos de Trabalho (WP's)			
Entradas			
Número	**Descrição**		**Suporta**
PO1-WP1	Plano estratégico de TI		PO9-01, 02
PO1-WP2	Plano tático de TI		PO9-01, 02
PO1-WP3	Portfólio de projetos de TI		PO9-01, 02
PO1-WP4	Portfólio de serviços de TI		PO9-01, 02
PO10-WP2	Plano de gerenciamento de riscos de projeto		PO9-01, 02
DS2-WP3	Riscos dos fornecedores		PO9-01, 02
DS4-WP1	Resultados de testes de contingência		PO9-01, 02
DS5-WP5	Ameaças de segurança e vulnerabilidades		PO9-01, 02
ME1-WP3	Tendências com base no histórico de riscos e eventos		PO9-01, 02
ME4-WP5	Apetite da organização pelo risco de TI		PO9-01, 02
Saídas			
Número	**Descrição**		**Suporta**
PO9-WP1	Avaliação do risco		PO9-01, 02
PO9-WP2	Comunicação do risco		PO9-01, 02
PO9-WP3	Orientações para a gestão de riscos relacionados à TI		PO9-01
PO9-WP4	Plano de ação para o tratamento dos riscos relacionados à TI		PO9-02

A partir do modelo de referência do processo apresentado na tabela 14, é possível identificar as práticas base e produtos de trabalho que suportam os resultados esperados no processo de avaliar e gerenciar riscos de TI.

Os BP's e WP's definem os indicadores de performance do processo. Segundo o ISACA (2011a), os WP's não devem ser considerados como uma lista do que cada organização deva ter, mas sim um exemplo, ou seja, um ponto de partida considerando a possibilidade dos possíveis WP's contribuírem para a finalidade do processo.

4.3.1.1. Níveis de capacidade do processo

O novo modelo de maturidade do COBIT está baseado na norma ISO/IEC 15504-2 e não mais no CMMI. Assim, os seis níveis de maturidade originais foram mantidos, porém com novas descrições e significados. Os níveis de maturidade são apresentados a seguir.

Tabela 15: Níveis de capacidade do COBIT 4.1 com base na ISO/IEC 15504-2 (ISACA, 20011a)

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	

Os níveis de capacidade incompleto, executado e gerenciado, tem como foco a visão/conhecimento de uma instância da organização, enquanto os níveis estabelecido, previsível e em otimização possuem seu foco na organização como um todo.

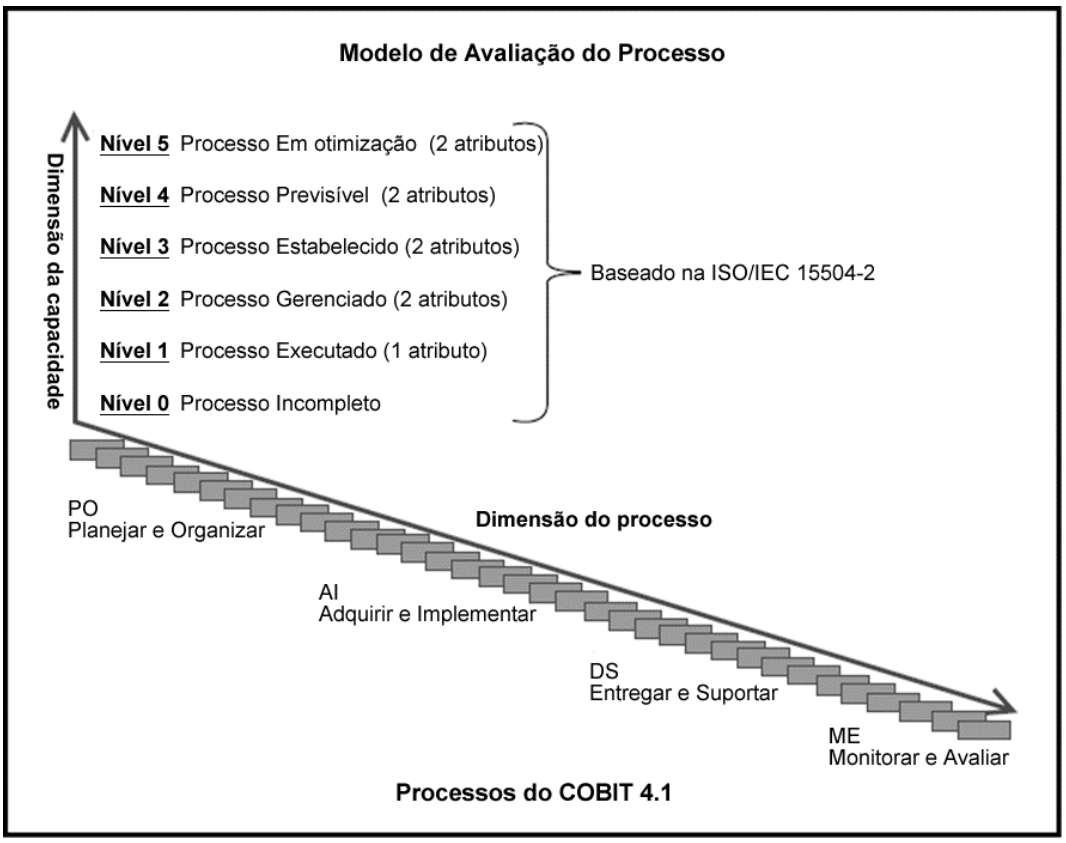


Figura 22: Modelo de Avaliação do Processo (ISACA, 20011a)

A figura 22 apresenta as duas dimensões do modelo de avaliação de processos: dimensão do processo e dimensão da capacidade. A dimensão do processo descreve os indicadores de performance do processo, que são diretamente mapeados aos processos definidos no Modelo de Referência de Processo.

4.3.1.2. Atributos do processo

Segundo o modelo de avaliação de processo do COBIT (ISACA, 2011b), a medição da capacidade está baseada em nove atributos de processo, também chamados de PA (do inglês *Process Atribute*). Os atributos de processo são utilizados para determinar se um processo alcançou uma determinada capacidade. Os atributos de processo são:

- PA1.1 Execução de processo (*process performance*)
- PA2.1 Gerência de execução (*performance management*)
- PA2.2 Gerência de produto de trabalho (*work product management*)
- PA3.1 Definição de processo (*process definition*)
- PA3.2 Implementação de processo (*process deployment*)
- PA4.1 Medição de processo (*process measurement*)

- PA4.2 Controle de processo (*process control*)
- PA5.1 Inovação de processo (*process inovation*)
- PA5.2 Otimização de processo (*continuous optimization*)

A norma ISO/IEC 15504-2 (ABNT, 2008b, p. 6) prevê que os atributos de processo sejam constituídos de forma a serem pontuados independentemente, o que não impede a existência de outros relacionamentos entre eles, ou seja, o alcance de um atributo pode estar ligado ao alcance de outro dentro da dimensão de capacidade. Para o modelo de avaliação de processos do COBIT (ISACA, 2011a), os atributos de processo utilizados no modelo não possuem relação direta entre si.

Cada atributo de processo está relacionado a uma capacidade específica e serve para determinar a capacidade de um processo. A figura abaixo demonstra a distribuição dos atributos de processos de acordo com os níveis de capacidade e pode ser aplicado a qualquer processo:

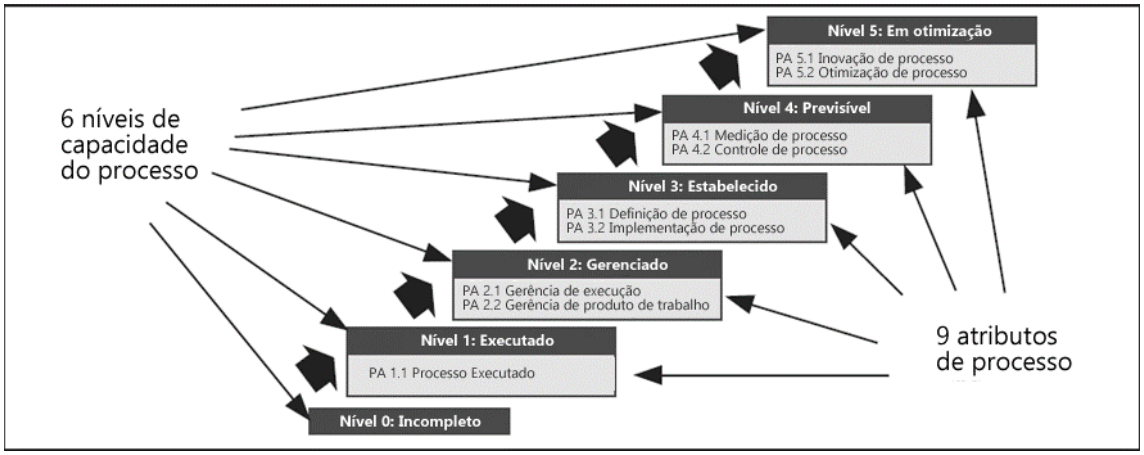


Figura 23: Atributos de processo x nível de capacidade do processo (ISACA, 20011b)

Observa-se que cada nível de capacidade do processo possui um conjunto de atributos de processo associados, onde o nível 0 (incompleto) não possui nenhum atributo de processo associado. O nível 1 (executado) utiliza o atributo de processo 1.1 (processo executado). No nível 2 (gerenciado) são utilizados, adicionalmente, dois novos atributos: 2.1 (gerência de execução) e 2.2 (gerência de produto de trabalho). Para o nível 3 (estabelecido) são incorporados dois outros atributos: 3.1 (definição do processo) e 3.2 (implementação do processo). Já o nível 4 (previsível) utiliza os atributos de processo 4.1 (medição do processo) e 4.2 (controle do processo). Por fim, o nível 5 (em otimização) utiliza os atributos 5.1 (inovação do processo) e 5.2 (otimização do processo).

4.3.1.3. Indicadores de avaliação

Os indicadores de avaliação são utilizados para verificar se os atributos de processos foram alcançados. Existem dois tipos de indicadores:

- Indicadores de capacidade do processo
- Indicadores de execução do processo

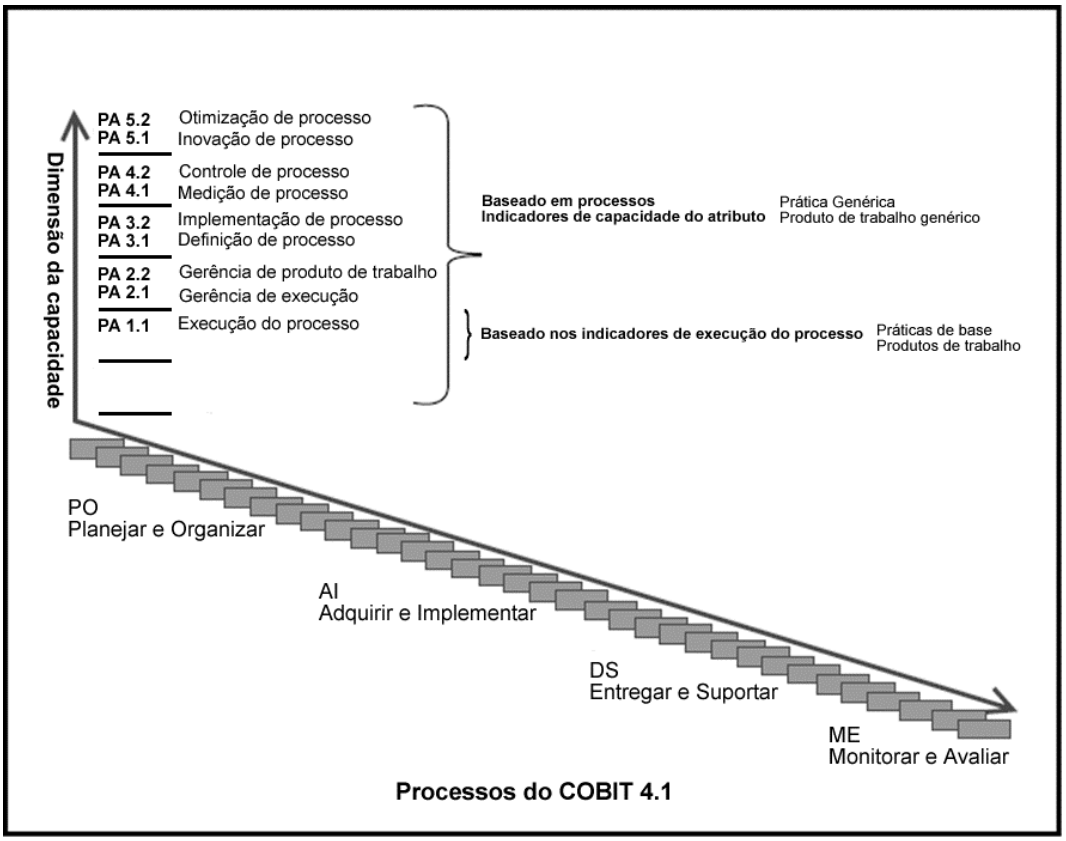


Figura 24: Indicadores de avaliação (ISACA, 20011a)

Os indicadores de capacidade do processo são genéricos para cada atributo de processo, aplicam-se aos níveis 1 a 5 e podem ser de dois tipos:

- Práticas genéricas (GP)
- Produto de trabalho genérico (GWP)

Já os indicadores de execução do processo variam de acordo com o processo analisado e servem para determinar se o processo está no nível 1. Vale ressaltar que os indicadores de execução se aplicam exclusivamente ao nível 1. Os indicadores de execução podem ser categorizados em:

- Práticas base
- Produtos de trabalho

4.3.1.4. Processo de auto avaliação

O programa de auto avaliação do COBIT prevê um processo simplificado de auto avaliação, não baseado em evidencias, sem necessidade de um avaliador e que pode ser feito pela própria TI, como precursora de uma avaliação mais formal. O objetivo da auto avaliação é identificar as lacunas nos processos que requerem uma avaliação formal, ajudando a TI a alcançar níveis de capacidade mais elevados com um custo reduzido (ISACA, 2011b)

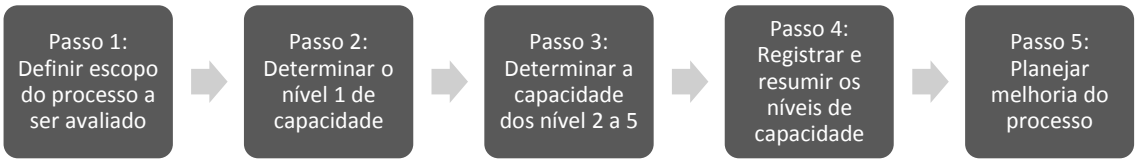


Figura 25: Processo de auto avaliação do COBIT (ISACA, 20011b)

O primeiro passo para a auto avaliação é decidir, dentre os 34 processos do COBIT 4.1, quais processos serão avaliados[4]. Deve ser considerado ainda nesta etapa qual o nível de capacidade alvo, que permitirá descrever quais os atributos de processo serão necessários para alcançar o alvo e ainda identificar quais impactos[5] nos objetivos de negócio que a organização estará submetida se um determinado nível de capacidade não for alcançado. O guia de auto avaliação do COBIT sugere uma planilha para registro do nível de capacidade alvo e o resultado efetivamente alcançado (anexo E)

No passo 2, deve-se determinar se o processo selecionado está no nível 1, ou seja, se é realmente executado e alcança seus resultados. Essa verificação é feita com o auxílio de uma planilha específica para cada processo com base nos critérios derivados do COBIT 4.1.

No passo 3, deve-se determinar se o processo selecionado está entre os níveis 2 e 5 de capacidade. Para isso, são avaliados critérios genéricos (não baseados no COBIT), aplicados a todos os demais processos. No passo 4 o resumo do resultado da avaliação é registrado, onde o nível de capacidade do processo é determinado. Por fim, no passo 5, deve ser desenvolvido um plano de ação considerando a auto avaliação, para a melhoria do processo.

[4] Neste estudo será avaliado o processo PO9: Avaliar e Gerenciar os Riscos de TI.

[5] A norma ABNT ISO/IEC 15504-4 (ABNT, 2008c) fornece uma tabela com as potenciais consequências de cada um dos atributos de processo.

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

Neste capítulo é apresentado 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 (produtos de trabalho), diminuindo a chance de respostas subjetivas e aumentando a precisão da avaliação.

O instrumento de avaliação original apresentava para cada nível de maturidade um conjunto de atributos de processo, que por sua 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 toma 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.

Tabela 16: 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 16, 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. Um protótipo do instrumento foi construído em Excel, sendo composto por quatro seções: 1) identificação; 2) avaliação; 3) resultados; 4) glossário. O instrumento desenvolvido permite o registro dos dados coletados junto à organização avaliada ao mesmo passo que automatiza o processo de avaliação. A seguir é exibido o formulário em Excel que materializa o instrumento de avaliação de maturidade em gestão de riscos de TI.

4.4.1. Seção I – Identificação

Esta seção é utilizada para a identificação da organização que está sendo avaliada, a pessoa responsável pela avaliação, a data em que a avaliação foi realizada, etc.

Tabela 17: Instrumento para coleta de dados e avaliação de maturidade em gestão de riscos de TI – Seção I – Identificação

Seção I - Identificação

Nome da organização:	
Data da avaliação:	___/___/_____
Nível de maturidade alvo:	
Responsável pelo processo de GR:	

4.4.2. Seção II – Avaliação

Esta seção apresenta o questionário a ser respondido pela organização, ondem constam todas as práticas e artefatos esperados, que suportam os critérios necessários para o cumprimento dos atributos de processo, que por sua vez serão utilizados para determinar o nível de maturidade do processo;

Tabela 18: Instrumento para coleta de dados e avaliação de maturidade em gestão de riscos de TI – Seção II – Avaliação

Seção II - Avaliação detalhada do processo

Nível	Atributo de processo	Critério (Resultados necessários para o alcance completo do atributo)	Tipo de evidência	ID	Prática ou Produto de Trabalho esperado	Completamente Implementado? (S/N)	*Comentários*	% alcançado	N (0-15%)	P (>15-50%)	L (>50-85%)	F (>85-100%)
Nível 1 - Executado	**PA 1.1 Execução do processo – o propósito do processo é atingido**	PO9-1 Uma estrutura de gestão de riscos está estabelecida e alinhada à estrutura de gestão de riscos da organização.	Prática Base	P09-BP1	Determinar alinhamento da gestão de riscos (ex. avaliar o risco)			0%	**X**			
				P09-BP2	Entender os objetivos estratégicos relevantes do negócio							
				P09-BP3	Entender os objetivos de processos relevantes do negócio							
				P09-BP4	Identificar os objetivos internos de TI relacionados à gestão de riscos, e estabelecer o contexto do risco							
				P09-BP5	Identificar os eventos associados a esses objetivos							
				P09-BP6	Avaliar os riscos associados aos eventos							
				P09-BP7	Avaliar respostas aos riscos							
			Produto de Trabalho	PO9-WP3	Orientações para a gestão de riscos relacionados à TI							
		PO9-2 Planos de ação para tratamento do risco são definidos e comunicados.	Prática Base	P09-BP8	Priorizar e planejar atividades de controle							
				P09-BP9	Aprovar e garantir fundos para os planos de ação de riscos							
			Produto de Trabalho	PO9-WP4	Plano de ação para o tratamento dos riscos relacionados à TI							
		PO9-01 e PO9-02	Prática Base									

Nível	Atributo de processo	Critério (Resultados necessários para o alcance completo do atributo)	Tipo de evidência	ID	Prática ou Produto de Trabalho esperado	Completamente Implementado? (S/N)	*Comentários*	% alcançado	N (0-15%)	P (>15-50%)	L (>50-85%)	F (>85-100%)
			Produto de Trabalho	PO1-WP1	Plano estratégico de TI							
				PO1-WP2	Plano tático de TI							
				PO1-WP3	Portfólio de projetos de TI							
				PO1-WP4	Portfólio de serviços de TI							
				PO10-WP2	Plano de gerenciamento de riscos de projeto							
				DS2-WP3	Riscos dos fornecedores							
				DS4-WP1	Resultados de testes de contingência							
				DS5-WP5	Ameaças de segurança e vulnerabilidades							
				ME1-WP3	Tendências com base no histórico de riscos e eventos							
				ME4-WP5	Apetite da organização pelo risco de TI							
				PO9-WP1	Avaliação do risco							
				PO9-WP2	Comunicação do risco							
Nível 2 - Gerenciado	**PA 2.1 Gerência de Execução – uma medida da extensão na qual a execução do processo é gerenciada**	a) Objetivos para a execução do processo são identificados	Prática Genérica	GP 2.1.1	**Identificar os objetivos** para a execução do processo.			0%	**X**			
			Produto de Trabalho Genérico	GWP 1	**Documentação do processo** deve delinear o escopo do processo.							
				GWP 2	**Plano do processo** deve fornecer detalhes dos objetivos de execução do processo.							

Nível	Atributo de processo	Critério (Resultados necessários para o alcance completo do atributo)	Tipo de evidência	ID	Prática ou Produto de Trabalho esperado	Completamente Implementado? (S/N)	*Comentários*	% alcançado	N (0-15%)	P (>15-50%)	L (>50-85%)	F (>85-100%)
		b) Execução do processo é planejada e monitorada	Prática Genérica	GP 2.1.2	**Planejar e monitorar a execução** do processo para cumprir os objetivos identificados.							
			Produto de Trabalho Genérico	GWP 2	**Plano do processo** deve fornecer detalhes dos objetivos de execução do processo.							
				GWP 9	**Registro de desempenho do processo** deve fornecer detalhes dos resultados. **Nota:** Neste nível, o registro do desempenho do processo pode estar na forma de relatórios, questões registradas e registros informais.							
		c) Execução do processo é ajustada para atender os planos	Prática Genérica	GP 2.1.3	**Ajustar a execução** do processo.							
			Produto de Trabalho Genérico	GWP 4	**Registro de qualidade** deve fornecer detalhes das ações tomadas quando o desempenho não é alcançado.							
		d) Responsabilidades e autoridades para execução do processo são definidas, atribuídas e comunicadas	Prática Genérica	GP 2.1.4	**Definir responsabilidade e autoridades** para a execução do processo.							
			Produto de Trabalho Genérico	GWP 1	**Documentação do processo** deve fornecer detalhes sobre a matriz de responsabilidades.							
				GWP 2	**Plano do processo** deve incluir detalhes do plano de comunicação do processo, bem como a experiência de desempenho do processo e habilidades requeridas.							

Nível	Atributo de processo	Critério (Resultados necessários para o alcance completo do atributo)	Tipo de evidência	ID	Prática ou Produto de Trabalho esperado	Completamente Implementado? (S/N)	*Comentários*	% alcançado	N (0-15%)	P (>15-50%)	L (>50-85%)	F (>85-100%)
		e) Recursos e informações necessárias para a execução do processo são identificados, disponibilizados, alocados e utilizados	Prática Genérica	GP 2.1.5	**Identificar e disponibilizar recursos** para executar o processo de acordo com o plano.							
			Produto de Trabalho Genérico	GWP 2	**Plano do processo** deve fornecer detalhes do plano de treinamento do processo e plano de recursos do processo.							
		f) Interfaces entre as partes envolvidas são gerenciadas para garantir tanto a comunicação efetiva quanto a atribuição clara das responsabilidades	Prática Genérica	GP 2.1.6	**Gerenciar as relações** entre as partes envolvidas.							
			Produto de Trabalho Genérico	GWP 1	**Documentação do processo** deve fornecer detalhes de indivíduos e grupos envolvidos (fornecedores, clientes e matriz de responsabilidades).							
				GWP 2	**Plano do processo** deve fornecer detalhes do plano de comunicação do processo.							
	PA 2.2 Gerência de produto de trabalho – uma medida da extensão na qual os produtos de trabalho são gerenciados apropriadamente. O produto de trabalho (ou saídas do processo) são definidos e controlados.	a) Requisitos para produtos de trabalho do processo são definidos	Prática Genérica	GP 2.2.1	**Definir os requisitos para os produtos de trabalho.**			0%	X			
			Produto de Trabalho Genérico	GWP 3	**Plano de qualidade** deve fornecer detalhes dos critérios de qualidade e estrutura e conteúdo do produto de trabalho							
		b) Requisitos para a documentação e controle dos produtos de trabalho são definidos	Prática Genérica	GP 2.2.2	**Definir os requisitos para documentação e controle** dos produtos de trabalho.							
			Produto de Trabalho Genérico	GWP 1	**Documentação do processo** deve fornecer detalhes dos controles (matriz de controles).							

Nível	Atributo de processo	Critério (Resultados necessários para o alcance completo do atributo)	Tipo de evidência	ID	Prática ou Produto de Trabalho esperado	Completamente Implementado? (S/N)	*Comentários*	% alcançado	N (0-15%)	P (>15-50%)	L (>50-85%)	F (>85-100%)
				GWP 3	**Plano de qualidade** deve fornecer detalhes do produto de trabalho, critérios de qualidade, documentação exigida e controle de mudanças.							
		c) Produtos de trabalho são identificados, documentados e controlados apropriadamente	Prática Genérica	GP 2.2.3	**Identificar, documentar e controlar** os produtos de trabalho.							
			Produto de Trabalho Genérico	GWP 3	**Plano de qualidade** deve fornecer detalhes do produto de trabalho, critérios de qualidade, documentação exigida e controle de mudanças.							
		d) Produtos de trabalho são revisados de acordo com o planejado e ajustados, quando necessário, para atender os requisitos	Prática Genérica	GP 2.2.4	**Identificar e ajustar os produtos de trabalho** para atender os requisitos definidos.							
			Produto de Trabalho Genérico	GWP 4	**Registro de qualidade** deve fornecer uma trilha de auditoria das revisões realizadas.							
Nível 3 - Estabelecido	**PA 3.1 Definição de processo – uma medida da extensão na qual um processo padrão é mantido para apoiar a implementação do processo definido.**	a) Um processo padrão, incluindo diretrizes apropriadas para sua adaptação, é definido para descrever os elementos fundamentais que devem ser incorporados num processo definido	Prática Genérica	GP 3.3.1	**Definir o processo padrão** que suportará a implantação dos processos definidos.			0%	X			
			Produto de Trabalho Genérico	**GWP 5**	**Políticas e normas devem fornecer detalhes dos objetivos organizacionais para o processo, padrões mínimos de desempenho, procedimentos padrão e requisitos para relatórios e monitoramento. A exigência de evidência neste nível não se refere apenas à existência**							

Nível	Atributo de processo	Critério (Resultados necessários para o alcance completo do atributo)	Tipo de evidência	ID	Prática ou Produto de Trabalho esperado	Completamente Implementado? (S/N)	*Comentários*	% alcançado	N (0-15%)	P (>15-50%)	L (>50-85%)	F (>85-100%)
					das políticas e normas, mas que elas sejam aplicadas em toda a organização.							
		b) A sequência e a interação do processo padrão com outros processos são determinadas	Prática Genérica	GP 3.1.2	**Determinar a sequência e interação entre os processos** para que eles funcionem como um sistema integrado de processos.							
			Produto de Trabalho Genérico	GWP 5	**Políticas e normas** devem fornecer um mapeamento do processo com detalhes dos processos padrão e sequências e interações esperadas. A exigência de evidência neste nível não se refere apenas à existência das políticas e normas, mas que elas sejam aplicadas em toda a organização.							
		c) Competências e papéis requeridos para execução do processo são identificadas como parte do processo padrão	Prática Genérica	GP 3.1.3	**Identificar os papéis e competências** para a execução do processo padrão.							
			Produto de Trabalho Genérico	GWP 5	**Políticas e normas** devem fornecer detalhes dos papéis e competências para realização. A exigência de evidência neste nível não se refere apenas à existência das políticas e normas, mas que elas sejam aplicadas em toda a organização.							

Nível	Atributo de processo	Critério (Resultados necessários para o alcance completo do atributo)	Tipo de evidência	ID	Prática ou Produto de Trabalho esperado	Completamente Implementado? (S/N)	*Comentários*	% alcançado	N (0-15%)	P (>15-50%)	L (>50-85%)	F (>85-100%)
		d) Infraestrutura e ambiente de trabalho requeridos para execução de um processo são identificados como parte do processo padrão	Prática Genérica	GP 3.1.4	**Identificar a infraestrutura e ambiente de trabalho necessários** para a execução do processo padrão.							
			Produto de Trabalho Genérico	GWP 5	**Políticas e normas** devem identificar as exigência mínimas de infraestrutura e ambiente de trabalho para a realização do processo. A exigência de evidência neste nível não se refere apenas à existência das políticas e normas, mas que elas sejam aplicadas em toda a organização.							
		e) Métodos apropriados para monitorar a eficácia e adequação dos processos são determinados	Prática Genérica	GP 3.1.5	**Determinar métodos adequados** para monitorar a eficácia e sustentabilidade do processo padrão, incluindo a garantia que critérios apropriados e dados necessários estão definidos, e estabelecendo a necessidade de realizar auditoria interna e análise crítica pela direção.							
			Produto de Trabalho Genérico	GWP 5	**Políticas e normas** devem fornecer detalhes os objetivos organizacionais para o processo, padrões mínimos de desempenho, procedimentos padrão e requisitos para relatórios e monitoramento. A exigência de evidência neste nível não se refere apenas à existência das políticas e normas, mas							

Nível	Atributo de processo	Critério (Resultados necessários para o alcance completo do atributo)	Tipo de evidência	ID	Prática ou Produto de Trabalho esperado	Completamente Implementado? (S/N)	*Comentários*	% alcançado	N (0-15%)	P (>15-50%)	L (>50-85%)	F (>85-100%)
					que elas sejam aplicadas em toda a organização.							
				GWP 4 / GWP 9	**Os registros da qualidade e registros de desempenho de processo** devem fornecer evidência das revisões realizadas.							
	PA 3.2 Implementação do processo – uma medida de extensão na qual o processo padrão é efetivamente implementado como um processo definido para atingir seus resultados.	a) Um processo definido é implementado com base em um processo padrão apropriadamente selecionado e/ou adaptado	Prática Genérica	GP 3.2.1	**Implantar processo definido** que satisfaça o contexto.			0%	**X**			
			Produto de Trabalho Genérico	GWP 5	**Políticas e normas** devem fornecer detalhes os objetivos organizacionais para o processo, padrões mínimos de desempenho, procedimentos padrão e requisitos para relatórios e monitoramento. A exigência de evidência neste nível não se refere apenas à existência das políticas e normas, mas que elas sejam aplicadas em toda a organização.							
		b) Os papéis, autoridades e responsabilidades requeridos para	Prática Genérica	GP 3.2.2	**Atribuir e comunicar papéis, responsabilidade e autoridades** para a execução do processo definido.							

Nível	Atributo de processo	Critério (Resultados necessários para o alcance completo do atributo)	Tipo de evidência	ID	Prática ou Produto de Trabalho esperado	Completamente Implementado? (S/N)	*Comentários*	% alcançado	N (0-15%)	P (>15-50%)	L (>50-85%)	F (>85-100%)
		execução do processo definido são atribuídos e comunicado	Produto de Trabalho Genérico	GWP 5	**Políticas e normas** devem fornecer detalhes os objetivos organizacionais para o processo, padrões mínimos de desempenho, procedimentos padrão e requisitos para relatórios e monitoramento. A exigência de evidência neste nível não se refere apenas à existência das políticas e normas, mas que elas sejam aplicadas em toda a organização.							
		c) As pessoas que executam o processo definido são competentes em termos de educação, treinamento e experiência apropriados	Prática Genérica	GP 3.2.3	**Garantir competências necessárias** para a execução do processo definido.							
			Produto de Trabalho Genérico	GWP 1	**Documentação do processo** deve fornecer detalhes sobre a matriz de responsabilidades.							
				GWP 2	**Plano do processo** deve incluir detalhes do plano de comunicação do processo, bem como a experiência de desempenho do processo e habilidades requeridas.							
		d) Recursos e informações requeridos para a execução do processo definido são disponibilizados, alocados e utilizados	Prática Genérica	GP 3.2.4	**Definir recursos e informação para apoiar a execução** do processo definido.							
			Produto de Trabalho Genérico	GWP 2	**Plano do processo** deve incluir detalhes do plano de comunicação do processo, bem como a experiência de desempenho do processo e habilidades requeridas.							

Nível	Atributo de processo	Critério (Resultados necessários para o alcance completo do atributo)	Tipo de evidência	ID	Prática ou Produto de Trabalho esperado	Completamente Implementado? (S/N)	*Comentários*	% alcançado	N (0-15%)	P (>15-50%)	L (>50-85%)	F (>85-100%)
		e) Infraestrutura e ambiente de trabalho requeridos para execução do processo definido são disponibilizados, gerenciados e mantidos	Prática Genérica	GP 3.2.5	**Fornecer infraestrutura adequada ao processo** para apoiar a execução do processo definido.							
			Produto de Trabalho Genérico	GWP 2	**Plano do processo** deve incluir detalhes do plano de comunicação do processo, bem como a experiência de desempenho do processo e habilidades requeridas.							
		f) Dados apropriados são coletados e analisados, constituindo uma base para o entendimento do comportamento do processo, para demonstrar a adequação e eficácia do processo, e avaliar onde pode ser feita a melhoria contínua do processo.	Prática Genérica	GP 3.2.6	**Coletar e analisar dados** sobre a execução do processo para demonstrar sua adequabilidade e eficácia.							
			Produto de Trabalho Genérico	GWP 4 / GWP 9	**Os registros da qualidade e registros de desempenho de processo** devem fornecer evidência de instrumentos das revisões realizadas para cada instância do processo.							
Nível 4 - Previsível	**PA 4.1 Medição de processo – uma medida que quantifica a utilização dos resultados de medições para garantir que a execução do**	a) Necessidades de informação de processo são estabelecidas para apoiar o alcance de metas de negócio definidas e relevantes	Prática Genérica	GP 4.1.1	**Identificar as necessidades de informação do processo**, em relação aos objetivos de negócio.			0%	**X**			
			Produto de Trabalho Genérico	GWP 6	**Plano de melhoria do processo** deve fornecer objetivos de melhoria do processo e ações de melhoria propostas.							

Nível	Atributo de processo	Critério (Resultados necessários para o alcance completo do atributo)	Tipo de evidência	ID	Prática ou Produto de Trabalho esperado	Completamente Implementado? (S/N)	*Comentários*	% alcançado	N (0-15%)	P (>15-50%)	L (>50-85%)	F (>85-100%)
	processo apoie o alcance de objetivos relevantes de desempenho para suportar o alcance das metas definidas para o negócio.	b) Objetivos de medição de processo são derivados de necessidades de informação de processo	Prática Genérica	GP 4.1.2	**Derivar os objetivos de medição do processo** a partir das necessidades de informação. Os objetivos de medição são baseados nos processos definidos.							
			Produto de Trabalho Genérico	GWP 7	**Plano de medição do processo** deve fornecer detalhes dos objetivos de medição propostos.							
		c) Objetivos quantitativos para o desempenho do processo são estabelecidos em apoio ao alcance de metas relevantes de negócio	Prática Genérica	GP 4.1.3	**Estabelecer objetivos quantitativos** para a execução dos processos definidos, de acordo como alinhamento entre processo e objetivos de negócio.							
			Produto de Trabalho Genérico	GWP 7	**Plano de medição do processo** deve fornecer detalhes da medição proposta de indicadores e métricas.							
		d) Medidas e frequências de medição são identificadas e definidas de forma alinhada com os objetivos de medição de processo e os objetivos quantitativos para o desempenho do processo	Prática Genérica	GP 4.1.4	**Identificar medidas de produtos e processos** que apoiam a realização dos objetivos quantitativos para execução do processo.							
			Produto de Trabalho Genérico	GWP 7	**Plano de medição do processo** deve fornecer detalhes das medidas propostas/indicadores, juntamente com procedimentos de coleta de dados e procedimentos analíticos.							
		e) Resultados da medição são coletados,	Prática Genérica	GP 4.1.5	**Coletar resultados de medição dos produtos e processos** através da							

Nível	Atributo de processo	Critério (Resultados necessários para o alcance completo do atributo)	Tipo de evidência	ID	Prática ou Produto de Trabalho esperado	Completamente Implementado? (S/N)	*Comentários*	% alcançado	N (0-15%)	P (>15-50%)	L (>50-85%)	F (>85-100%)
		analisados e comunicados para monitorar a extensão na qual os objetivos quantitativos para o desempenho do processo são alcançados			execução dos processos definidos.							
			Produto de Trabalho Genérico	GWP 7	**Plano de medição do processo** deve fornecer detalhes dos procedimentos analíticos propostos.							
				GWP 9	**Registro de desempenho do processo** deve fornecer detalhes das medições coletadas e analisadas.							
		f) Resultados de medição são usados para caracterizar o desempenho do processo.	Prática Genérica	GP 4.1.6	**Usar os resultados da medição definida** para monitorar e verificar o alcance dos objetivos de execução dos processos.							
			Produto de Trabalho Genérico	GWP 9	**Registro de desempenho do processo** deve fornecer detalhes das medições coletadas e analisadas.							
	PA 4.2 Controle de processo – uma medida na qual o processo é gerenciado quantitativamente, resultando em um processo estável, capaz e previsível dentro de limites definidos.	a) Técnicas de análise e controle são determinadas e aplicadas onde apropriado	Prática Genérica	GP 4.2.1	**Determinar as técnicas de análise e controle** apropriadas para o controle da execução do processo.			0%	**X**			
			Produto de Trabalho Genérico	GWP 1	**Documentação do processo deve fornecer detalhes dos controles (matriz de controles).**							
				GWP 8	**Plano de controle do processo** deve especificar para cada processo a abordagem de medição.							
		b) Limites de controle de variação são	Prática Genérica	GP 4.2.2	**Definir parâmetros** adequados para controlar o desempenho do processo.							

Nível	Atributo de processo	Critério (Resultados necessários para o alcance completo do atributo)	Tipo de evidência	ID	Prática ou Produto de Trabalho esperado	Completamente Implementado? (S/N)	*Comentários*	% alcançado	N (0-15%)	P (>15-50%)	L (>50-85%)	F (>85-100%)
		estabelecidos para o desempenho normal do processo	Produto de Trabalho Genérico	GWP 8	**Plano de controle do processo** deve especificar para cada processo limites de desempenho normal.							
		c) Dados de medição são analisados para identificar causas especiais de variação	Prática Genérica	GP 4.2.3	**Analisar resultados da medição do processo e produto** para identificar variações na execução do processo.							
			Produto de Trabalho Genérico	GWP 9	**Registro de desempenho do processo** deve fornecer detalhes das medições coletadas e analisadas.							
		d) Ações corretivas são tomadas para tratar as causas especiais de variação	Prática Genérica	GP 4.2.4	**Identificar e implementar ações corretivas** para tratar de causas atribuíveis.							
			Produto de Trabalho Genérico	GWP 9	**Registro de desempenho do processo** deve fornecer detalhes das medições coletadas e analisadas e ações de correção tomados.							
		e) Limites de controle são restabelecidos (se necessário) seguindo a ação corretiva	Prática Genérica	GP 4.2.5	**Estabelecer novamente os limites de controle** após as ações corretivas.							
			Produto de Trabalho Genérico	GWP 8	**Plano de controle do processo** deve especificar para cada processo limites de desempenho normal.							
Nível 5 - Em otimização	**PA 5.1 Inovação de processo – uma medida na qual as mudanças ocorridas no processo são identificadas através de análises das causas comuns**	a) Objetivos de melhoria de processo são definidos para o processo em questão a fim de apoiar os objetivos de negócios relevantes	Prática Genérica	GP 5.1.1	**Definir os objetivos de melhoria do processo** para os processos que apoiam os objetivos relevante de negócio.			0%	**X**			
			Produto de Trabalho Genérico	GWP 6	**Plano de melhoria do processo** deve fornecer objetivos de melhoria do							

Nível	Atributo de processo	Critério (Resultados necessários para o alcance completo do atributo)	Tipo de evidência	ID	Prática ou Produto de Trabalho esperado	Completamente Implementado? (S/N)	*Comentários*	% alcançado	N (0-15%)	P (>15-50%)	L (>50-85%)	F (>85-100%)
	de variação em sua execução e da investigação de abordagens inovadoras para a definição e implementação do processo.				processo e ações de melhoria propostas.							
		b) Dados apropriados são analisados para identificar as causas comuns das variações na execução do processo	Prática Genérica	GP 5.1.2	**Definir os objetivos de melhoria do processo** para os processos que apoiam os objetivos relevantes de negócio.							
			Produto de Trabalho Genérico	GWP 9	**Registro de desempenho do processo** deve fornecer detalhes das medições coletadas e analisadas.							
		c) Dados apropriados são analisados para identificar oportunidades para melhores práticas de inovação	Prática Genérica	GP 5.1.3	**Analisar dados de medição do processo** para identificar variações reais e potenciais na execução do processo.							
			Produto de Trabalho Genérico	GWP 6	**Plano de melhoria do processo** deve fornecer detalhes de análises contra melhores práticas.							
		d) Oportunidades de melhoria derivadas de novas tecnologias e novos conceitos de processo são identificadas	Prática Genérica	GP 5.1.4	**Criar oportunidades de melhoria dos processos** através de novas tecnologias e conceitos dos processos.							
			Produto de Trabalho Genérico	GWP 6	**Plano de melhoria do processo** deve fornecer detalhes sobre a análise de oportunidades de melhoria da tecnologia.							
		e) Uma estratégia é estabelecida visando atingir os objetivos de melhoria do processo.	Prática Genérica	GP 5.1.5	**Definir uma estratégia de implementação** baseado na melhoria de visão e objetivos de longo prazo.							
			Produto de Trabalho Genérico	GWP 6	**Plano de melhoria do processo** deve fornecer detalhes da estratégia de							

Nível	Atributo de processo	Critério (Resultados necessários para o alcance completo do atributo)	Tipo de evidência	ID	Prática ou Produto de Trabalho esperado	Completamente Implementado? (S/N)	*Comentários*	% alcançado	N (0-15%)	P (>15-50%)	L (>50-85%)	F (>85-100%)
					implementação para melhoria dos processos.							
	PA 5.2 Otimização de processo – uma medida na qual as mudanças na definição, gerenciamento e execução do processo resultam em um impacto eficaz, que atende aos objetivos relevantes de melhoria do processo.	a) O impacto de todas as mudanças propostas é avaliado em relação aos objetivos do processo definido e do processo padrão	Prática Genérica	GP 5.2.1	**Avaliar o impacto de cada alteração proposta** contra os objetivos dos processos padrão e definido.			0%	**X**			
			Produto de Trabalho Genérico	GWP 6	**Plano de melhoria do processo** deve fornecer detalhes sobre a abordagem da qualidade do projeto de melhoria de processo necessário.							
		b) A implementação de todas as mudanças acordadas é gerenciada para garantir que qualquer mau funcionamento da execução do processo seja compreendido e ações sejam tomadas	Prática Genérica	GP 5.2.2	**Gerenciar a implementação de alterações aceitas** das áreas selecionadas dos processos padrão e definido.							
			Produto de Trabalho Genérico	GWP 6	**Plano de melhoria do processo** deve fornecer detalhes sobre a estratégia de implementação de melhoria de processos e evidências de mudanças em: - Documentação do processo (GWP 1) - Plano de qualidade (GWP 3) - Políticas e normas (GWP 5)							
		c) A eficácia da mudança do processo, com base na execução real, é avaliada com relação aos requisitos definidos para o produto e aos objetivos do processo, visando	Prática Genérica	GP 5.2.3	**Avaliar a eficácia da alteração do processo** contra o desempenho do processo, capacidade dos objetivos e objetivos do negócio.							
			Produto de Trabalho Genérico	GWP 6	**Plano de melhoria do processo** deve fornecer detalhes sobre a abordagem da qualidade do projeto de							

Nível	Atributo de processo	Critério (Resultados necessários para o alcance completo do atributo)	Tipo de evidência	ID	Prática ou Produto de Trabalho esperado	Completamente Implementado? (S/N)	*Comentários*	% alcançado	N (0-15%)	P (>15-50%)	L (>50-85%)	F (>85-100%)
		determinar se os resultados são devido a causas comuns ou especiais.			melhoria de processo necessário.							

4.4.3. Seção III - Resultados

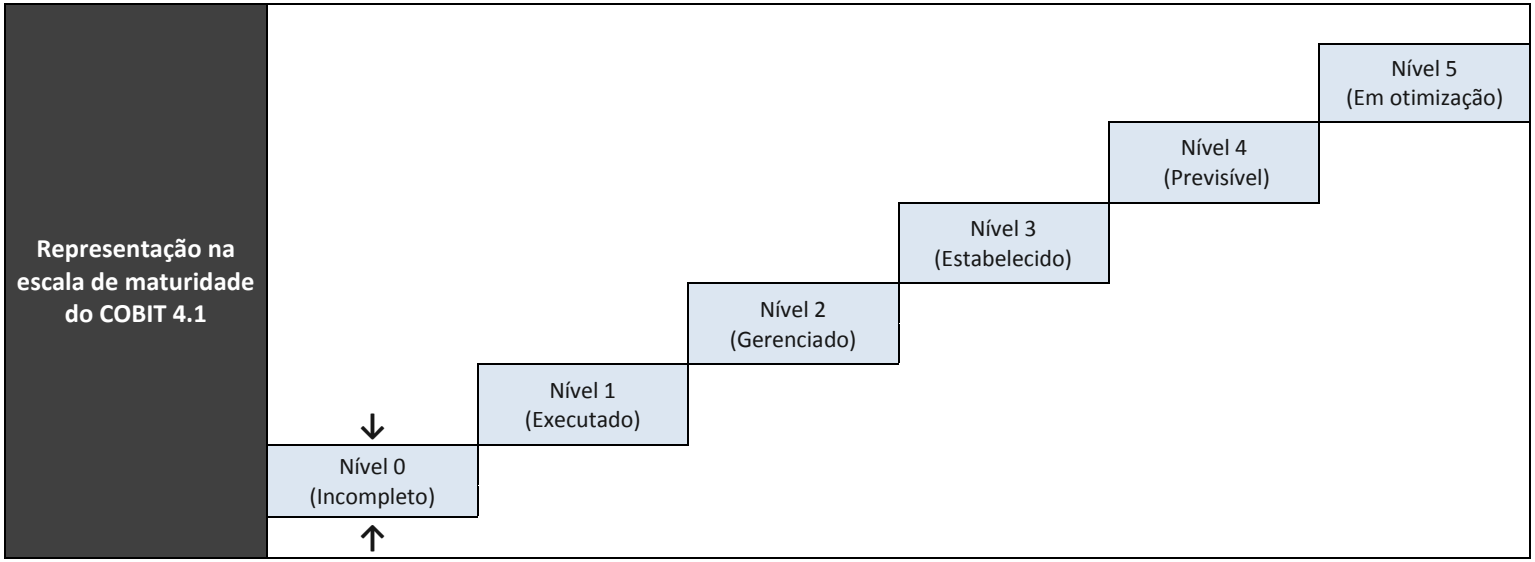
Nesta seção são apresentados os resultados alcançados de forma detalhada, ou seja, quais são práticas e produtos de trabalho existentes na organização, o quanto cada atributo de processo está sendo executado, o nível de maturidade do processo de gestão de riscos, etc.

Tabela 19: Instrumento para coleta de dados e avaliação de maturidade em gestão de riscos de TI – Seção III – Resultados

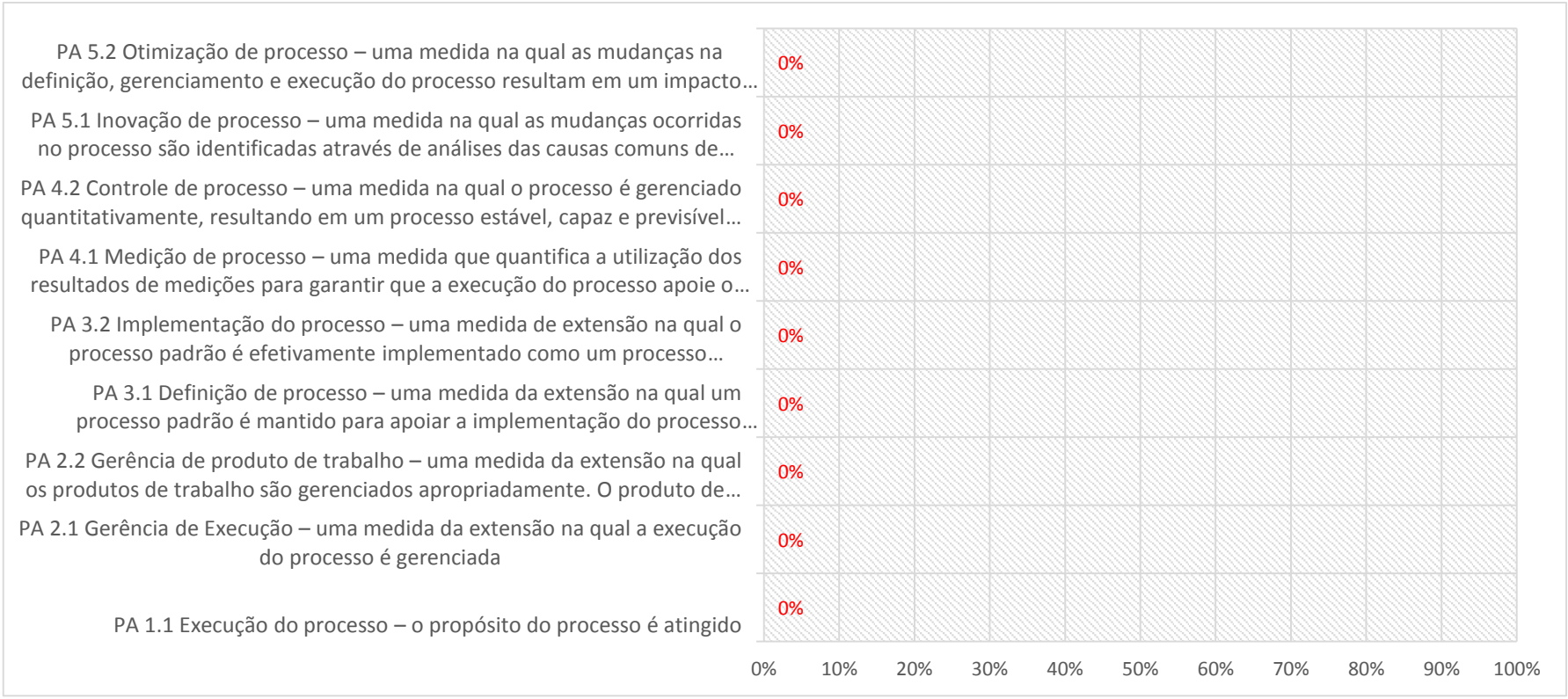
III - Resultados

Nome da organização:	
Data da avaliação:	___/___/_____
Responsável pelo processo de GR:	
Nome do processo no COBIT 4.1:	**Avaliar e Gerenciar os Riscos de TI**
Nível de maturidade alvo:	

Avaliação da capacidade do processo segundo os critérios	Nível 0	Nível 1	Nível 2		Nível 3		Nível 4		Nível 5	
		PA 1.1 (Execução de processo)	PA 2.1 (Gerência de execução)	PA 2.2 (Gerência de produto de trabalho)	PA 3.1 (Definição de processo)	PA 3.2 (Implementação de processo)	PA 4.1 (Medição de processo)	PA 4.2 (Controle de processo)	PA 5.1 (Inovação de processo)	PA 5.2 (Otimização de processo)
		N	N	N	N	N	N	N	N	N
	↑									



Nível de maturidade alcançado:	**Nível 0 - Incompleto**
Descrição do nível de maturidade do processo avaliado:	*Não implementado ou pouca/nenhuma evidência para um alcance sistemático do propósito do processo.*



4.4.4. Seção IV – Glossário

Por fim, a seção IV apresenta uma breve descrição dos principais termos utilizados na seção II (avaliação), cujo entendimento é indispensável para uma correta avaliação.

Tabela 20: Instrumento para coleta de dados e avaliação de maturidade em gestão de riscos de TI – Seção IV – Glossário

IV – Glossário

Atributo de processo	*Uma característica mensurável de capacidade de processo aplicável a qualquer processo.*
Capacidade alvo	*Capacidade de processo que o patrocinador da determinação de capacidade de processo julga que representará um risco de processo aceitável à implementação com sucesso do requisito específico.*
F	*Indica que o propósito do atributo de processo foi completamente atingido (> 85% a 100% de alcance)*
L	*Indica que o propósito do atributo de processo foi amplamente atingido (> 50% a 85% de alcance)*
N	*Indica que o propósito do atributo de processo não foi alcançado (0 a 15% de alcance)*
P	*Indica que o propósito do atributo de processo foi parcialmente atingido (> 15% a 50% de alcance)*
Prática base	*Uma atividade que, quando executada de forma consistente, contribui com o alcance do propósito do processo específico.*
Processo definido	*Um processo que é gerenciado (planejado, monitorado e ajustado) e adaptado a partir do conjunto de processos padronizados da organização de acordo com as orientações de adaptação da organização.*
Processo padrão	*Conjunto de definições dos processos básicos que orientam todos os processos de uma organização.*
Processo	*Conjunto de atividades que se inter-relacionam ou que interagem entre si, que transforma entradas em saídas.*
Produto de Trabalho	*Um artefato associação com a execução de um processo. Pode ser, por exemplo, um documento.*

4.4.5. Aferição da maturidade em gestão de riscos de TI

As seções I, II, III e IV do instrumento de avaliação apresentadas nos itens 3.4.1, 3.4.2, 3.4.3 e 3.4.4, foram construídas com apoio do software Excel, onde todos os resultados apresentados na seção III – resultados – são calculados de forma automatizada segundo os critérios definidos pelo modelo de referência do COBIT, que por sua vez se baseia no relatório técnico ISO/IEC 15504-7 (avaliação da maturidade de uma organização).

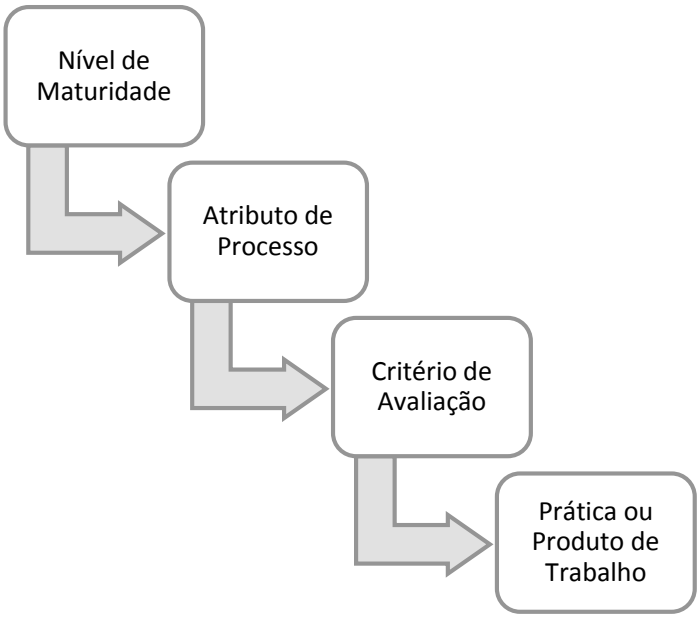


Figura 26: Agrupamento dos elementos de avaliação de maturidade

A figura 26 apresenta a forma como os elementos utilizados na avaliação estão agrupados. Um nível de maturidade pode ter um ou mais atributos de processos associados, que por sua vez possui um conjunto de critérios de avaliação. Esses critérios possuem Práticas e Produtos de Trabalho, que serão os elementos efetivamente avaliados.

Não seção I são registradas informações sobre a instituição e sobre a pessoa responsável pelo processo de gestão de riscos. A avaliação é feita com base nas respostas registradas na seção II, 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 é calculado o índice de capacidade de cada um dos atributos de processo. Para isso, é utilizada a seguinte fórmula:

$$ICAP = \frac{QRA}{TQA} * 100$$

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 composto pelos seguintes valores:

Tabela 21: Nível de capacidade dos atributos de processo (ISACA, 20011a, 2011b)

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 evidencia 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 22: Requisitos para pontuação em um nível de capacidade (ISACA, 20011b)

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.

4.5. Especificação dos Requisitos para Definição de Ferramentas Automatizadas

Outro produto esperado no objetivo 3 é a especificação dos requisitos para a definição de uma ferramenta automatizada para apoio ao processo de avaliação de maturidade em gestão de riscos de TI. Segundo a norma ISO 29148, o termo requisito pode ser entendido como uma declaração que traduz ou expressa uma necessidade e suas restrições e condições associadas. (ISO, 2011), podendo expressar necessidades em vários níveis. Desta forma, os requisitos para a construção de uma ferramenta automatizada para avaliação de maturidade em gestão de riscos de TI estão descritos a seguir:

4.5.1. Introdução

Este documento tem por finalidade apresentar os requisitos para a definição de um sistema de apoio ao processo de avaliação de maturidade em gestão de riscos de TI.

4.5.2. Referências

a) COBIT *Process Assessment Model (PAM);*
b) COBIT *Self-assessment Guide;*
c) ISO/IEC 15504 Tecnologia da informação – Avaliação de processo;
d) Modelo de Acessibilidade de Governo Eletrônico (e-MAG) versão 3.0;
e) Padrões de interoperabilidade de governo eletrônico (e-Ping) versão 2014;
f) Política de Segurança da Informação e Comunicações da Fiocruz e Normas Complementares.

4.5.3. Posicionamento

4.5.3.1. Descrição do problema

O problema	• Ausência de ferramentas para apoio ao processo de avaliação de maturidade em gestão de riscos de TI;
Afeta	• Coordenação de Gestão de Tecnologia da Informação; • Áreas de TI das unidades da Fiocruz;
O seu impacto é	• Demora na coleta de dados; • Erros nos dados coletados;

	• Dificuldade e demora na consolidação dos dados;
Benefícios com a solução	• Diminuir o tempo necessário para a coleta de dados junto às áreas de TI das unidades da Fiocruz; • Facilitar a consolidação dos dados; • Apoiar o cálculo da capacidade dos atributos de processo; • Determinar, sem erros, a definição dos níveis de maturidade;

4.5.3.2. Situação atual

Atualmente não existe nenhuma ferramenta desenvolvida para apoiar a avaliação de maturidade em gestão de riscos em TI. Os requisitos aqui apresentados fazem parte de uma proposta acadêmica, que propõe um instrumento de avaliação avançado, a partir das proposições do modelo de avaliação de processo do COBIT, alinhado à norma ISO/IEC 15504.

4.5.4. Interessados

Identificação	Descrição	Unidade
Gestor de TI das unidades da Fiocruz	Responsável pelo serviço de TI junto à unidade onde existe um processo de gestão de riscos de TI implantado.	Biomanguinhos, CECAL, COC, ENSP, EPSJV, Farmanguinhos, IAM, ICC, ICICT, IFF, IGM, ILMD, INCQS, IOC, IPEC e IRR, além dos escritórios da Fiocruz no Ceará, Piauí, Rondônia e Mato Grosso do Sul.
Coordenador de TI da Fiocruz	Responsável pela coordenação do serviço de TI em nível institucional e um dos interessados no projeto de avaliação de maturidade em gestão de riscos de TI.	CGTI

4.5.5. Visão geral do produto

4.5.5.1. Solução proposta

A solução proposta tem como principais características ser um sistema baseado no uso da Internet para coleta de dados junto às unidades da Fiocruz através de um questionário sobre a prática de gestão de riscos na unidade, trançando o nível de capacidade da unidade e o nível institucional de maturidade em gestão de riscos de TI.

4.5.5.2. Requisitos funcionais

Id	Descrição
RF_MGR01	O sistema deve fornecer um questionário para coleta de dados junto às unidades.
RF_MGR02	O sistema deve permitir ao entrevistado indicar um nível de maturidade alvo.
RF_MGR03	O sistema deve calcular o nível de capacidade das unidades com base nas respostas do questionário.
RF_MGR04	O sistema deve calcular o nível de maturidade institucional em gestão de riscos com base nas respostas das unidades.
RF_MGR05	O sistema deve processar os resultados e permitir uma comparação entre a unidade e a instituição, caso seja acessado pela unidade.
RF_MGR06	O sistema deve processar os resultados e permitir uma comparação entre as unidades e a instituição, caso seja acessado pela CGTI.
RF_MGR07	O sistema deve manter o histórico das avaliações de maturidade.
RF_MGR08	O sistema deve expressar os níveis de maturidade de acordo com a escala abaixo: Nível 0 – Incompleto; Nível 1 – Executado; Nível 2 – Gerenciado; Nível 3 – Estabelecido; Nível 4 – Previsível; Nível 5 – Em otimização;
RF_MGR09	O sistema deve manter uma associação entre atributos de processos avaliados e os níveis de maturidade, conforme abaixo: Nível 1 – PA1.1 Execução de processo; Nível 2 – PA2.1 Gerência de execução e PA2.2 Gerência de produto de trabalho; Nível 3 – PA3.1 Definição de processo e PA3.2 Implementação de processo; Nível 4 – PA4.1 Medição de processo e PA4.2 Controle de processo;

	Nível 5 – PA5.1 Inovação de processo e PA5.2 Otimização de processo.
RF_MGR10	O sistema deve calcular o indicador de execução do processo a partir da seguinte fórmula: $$\%\ atingido = \frac{Qtd\ de\ artefatos\ existentes}{Total\ de\ artefatos\ requeridos} X\ 100$$
RF_MGR11	O sistema deve calcular o nível de capacidade para cada atributo de processo.
RF_MGR12	O sistema deve apresentar nível de capacidade N (não atingido) quando um atributo de processo alcançar um indicador de execução menor ou igual a 15 % de alcance.
RF_MGR13	O sistema deve apresentar nível de capacidade P (parcialmente atingido) quando um atributo de processo alcançar um indicador de execução maior que 15% e até 50% de alcance.
RF_MGR14	O sistema deve apresentar nível de capacidade L (amplamente atingido) quando um atributo de processo alcançar um indicador de execução maior que 50% e até 85% de alcance.
RF_MGR15	O sistema deve apresentar nível de capacidade F (completamente atingido) quando um atributo de processo alcançar um indicador de execução maior que 85%.
RF_MGR16	O sistema deve processar os atributos de processos para determinar o nível de capacidade da unidade.
RF_MGR17	O sistema deve processar inicialmente o atributo de processo PA1.1 (referente ao nível de capacidade 1) e indicar ser este o nível alcançado, caso apresente minimamente a classificação L (amplamente atingido) ou F (completamente atingido).
RF_MGR18	O sistema deve processar os atributos de processo dos demais níveis de capacidade de forma crescente (nível 2, nível 3, e assim por diante)
RF_MGR19	O sistema deve indicar estar em um determinado nível de capacidade caso todas as condições a seguir forem cumpridas: a) O nível analisado seja o nível 2, 3, 4 ou 5; b) A classificação alcançada seja minimamente a L (amplamente atingido) ou F (completamente atingido); c) Atributos de processo associados aos níveis inferiores tenham obtido obrigatoriamente a classificação F (completamente atingido).
RF_MGR20	O sistema deve indicar nível de capacidade 0 (incompleto) caso o atributo de processo do nível 1 (PA1.1) não tenha alcançado a

	classificação mínima L (amplamente atingido) ou F (completamente atingido).

4.5.6. Especificação suplementar

4.5.6.1. Compatibilidade

Devem ser observadas as recomendações da Arquitetura e-PING v. 2014, que define os padrões de interoperabilidade de governo eletrônico em áreas como: interconexão, segurança, meios de acesso, organização e intercâmbio de informações.

4.5.6.2. Usabilidade

Devem ser observadas as recomendações para o processo de acessibilidade dos sítios e portais do governo brasileiro, constantes no Modelo de Acessibilidade de Governo Eletrônico (e-MAG) versão 3.0.

4.5.6.3. Segurança

Deve ser observada a Política de Segurança da Informação e Comunicações da Fiocruz, em especial a Norma Complementar 006, que dispõe de orientações sobre aquisição, desenvolvimento e manutenção de sistemas de informação.

4.6. Aplicação do Instrumento para Validação dos Requisitos

Para validação do instrumento de avaliação proposto, apresentado no capítulo 3.3.2, foi construída uma planilha eletrônica em Excel que automatiza o processo de cálculo do percentual alcançado pelos atributos de processo, determinando também o nível de maturidade alcançado. Os resultados da aplicação do instrumento são apresentados em duas perspectivas: Análise da aplicação do instrumento de avaliação de maturidade e resultados obtidos pela aplicação do instrumento de maturidade.

4.6.1. Análise da aplicação do instrumento de avaliação de maturidade

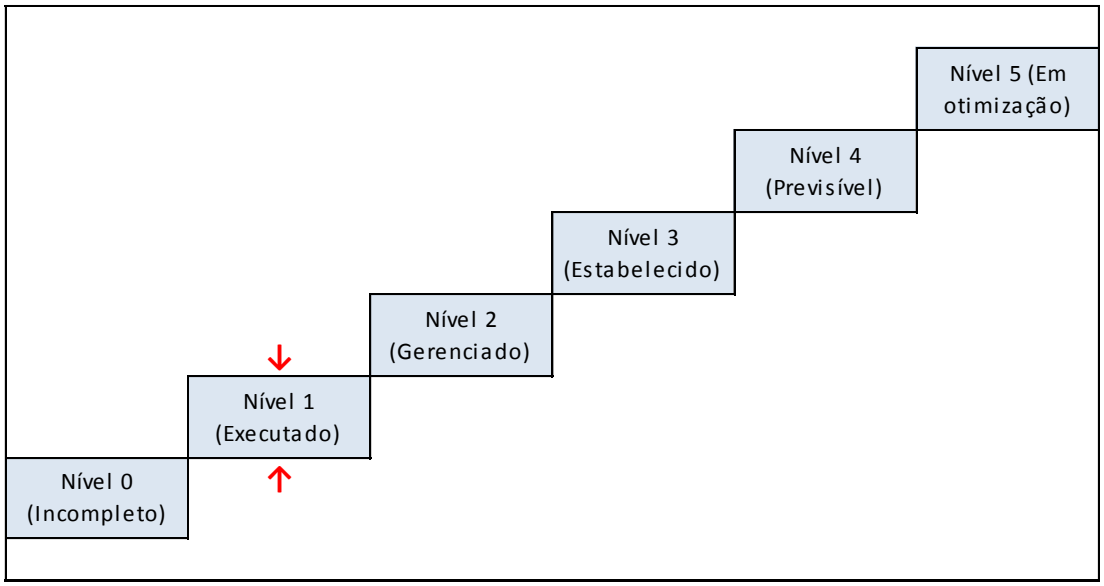
O instrumento foi aplicado na Coordenação de Gestão de Tecnologia da Informação da Fiocruz (CGTI) para avaliação do seu processo de gestão de riscos de TI. O instrumento desenvolvido em Excel foi encaminhado a um profissional que conhecia em detalhes o processo de gestão de riscos de TI na CGTI e que apontou

a necessidade de alguns ajustes no instrumento. Em relação aos requisitos implementados no instrumento, não foi identificado qualquer problema em relação aos dados coletados ou cálculos realizados com as diversas variáveis envolvidas, tornando válido os requisitos especificados e o instrumento desenvolvido. Segundo relatado pelo profissional que respondeu às questões no formulário, houve dificuldade na compreensão de alguns termos utilizados no formulário a partir dos critérios de nível 2. Foi identificado que esses critérios são oriundos do modelo de avaliação de processos do COBIT (baseados na norma ISO/IEC 15504-2). Outra dificuldade encontrada foi que os critérios de avaliação referenciavam por vezes produtos de trabalho exigidos pelo modelo de referência do COBIT. Como o processo de gestão de riscos não foi definido com bases nesses artefatos, não fazia sentido realizar uma avaliação exigindo como evidencia aqueles produtos de trabalho. Tendo em vista os problemas relatados, foram feitas algumas alterações no instrumento e no processo de avaliação. Uma das alterações foi a inclusão de uma seção IV no protótipo do instrumento com a definição de alguns termos necessários para o correto entendimento dos critérios de avaliação, utilizados na seção II (veja item 4.4.2).

4.6.2. Resultados obtidos pela aplicação do instrumento de maturidade

Os principais resultados são descritos a seguir:

Figura 27: Nível de maturidade em gestão de riscos de TI alcançado pela CGTI



Após a aplicação do instrumento de avaliação foi possível identificar que a CGTI se encontra no nível 1 de maturidade (executado), sendo possível afirmar que

o processo atinge o seu propósito. Para uma análise mais detalhada do resultado, faz-se necessário consultar os resultados das avaliações dos atributos de processo.

Figura 28: Resultados da avaliação dos atributos de processo

Nível 0	Nível 1	Nível 2		Nível 3		Nível 4		Nível 5	
	PA 1.1 (Execução de processo)	PA 2.1 (Gerência de execução)	PA 2.2 (Gerência de produto de trabalho)	PA 3.1 (Definição de processo)	PA 3.2 (Implementação de processo)	PA 4.1 (Medição de processo)	PA 4.2 (Controle de processo)	PA 5.1 (Inovação de processo)	PA 5.2 (Otimização de processo)
	L	L	P	P	L	L	N	P	P

Conforme pode ser visto na figura 28, o atributo de processo PA 1.1, responsável pelos critérios de execução de processo, recebeu uma classificação L, o que significa que seus critérios foram amplamente alcançados.

Observa-se ainda que o nível 2 de maturidade (Gerenciado) é composto por dois atributos de processo PA 2.1 (Gerência da Execução) e PA 2.2 (Gerência de Produto de Trabalho), onde o primeiro foi amplamente atingido (L) e o segundo parcialmente atingido (P). Vale ressaltar que para uma organização alcançar um determinado nível de maturidade, esta deve obter minimamente uma classificação L (amplamente atingido) ou ainda P (plenamente atingido) no nível alvo e uma avaliação F para os atributos de processo dos níveis inferiores (quando existirem).

O nível 3 de maturidade (Estabelecido) é composto por dois atributos de processo PA 3.1 (Definição do Processo) e PA 3.2 (Implementação do Processo), onde o primeiro foi parcialmente atingido (P) e o segundo amplamente atingido (L).

O nível 4 de maturidade (Previsível) também é composto por dois atributos de processo PA 4.1 (Medição de Processo) e PA 4.2 (Controle de Processo). Embora o objetivo do atributo de processo PA 4.1 tenha sido amplamente atingido, o atributo de processo PA 3.2 não teve seu objetivo atingido (N).

Por fim, o nível 5 de maturidade (Em otimização), composto pelos atributos de processo PA 5.1 (Inovação de Processo) e 5.2 (Otimização de Processo), obtiveram uma classificação P, ou seja, cumprem de forma parcial seus objetivos.

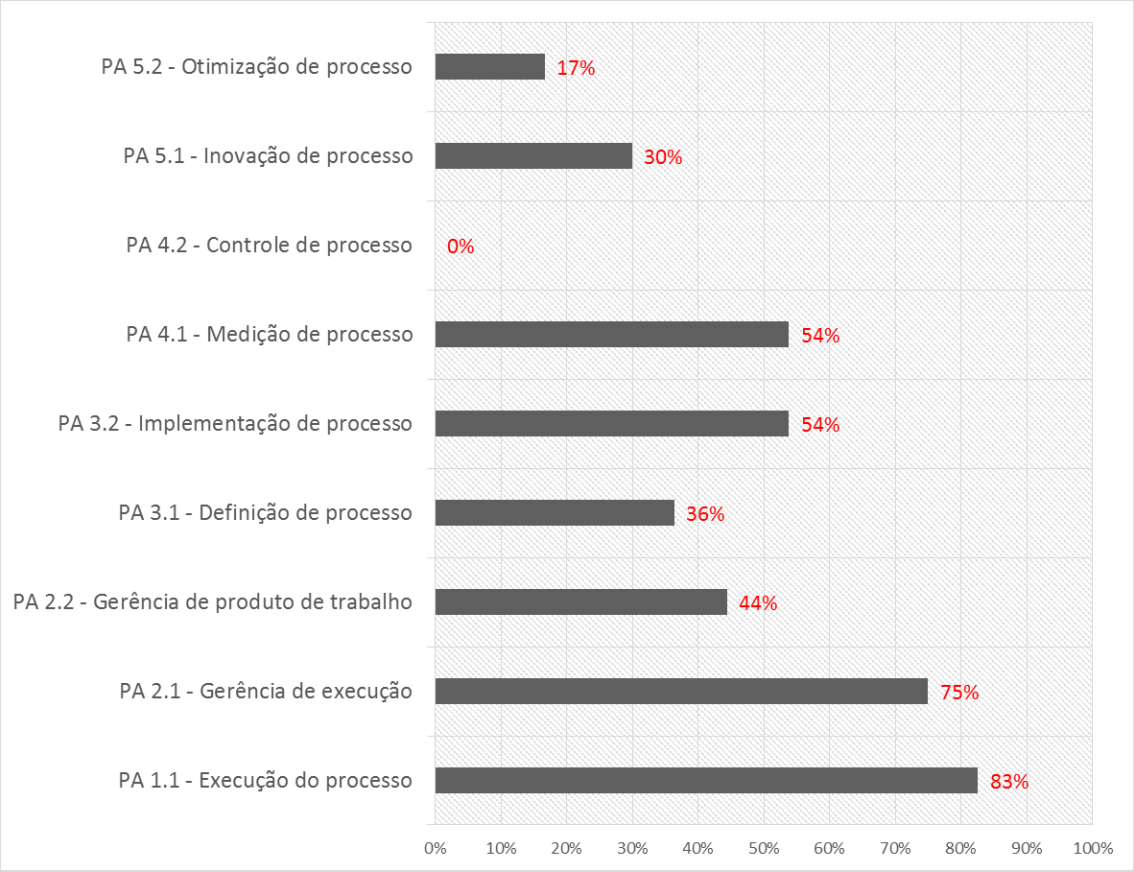


Figura 29: Percentual alcançado pelos atributos de processo

A figura 29 apresenta o percentual alcançado por cada atributo de processo. É possível observar que os atributos de processos referente aos níveis de maturidade mais baixos, se encontram mais consolidados, pois possuem uma maior aderência aos critérios avaliados. Da mesma forma, os níveis de maturidade mais elevados possuem um grau de aderência menor aos critérios de avaliação. Vale ressaltar ainda que durante a avaliação não foram encontradas evidencias que demonstrassem as práticas ou produtos de trabalho sugeridos para o atributo de processo PA 4.2 – Controle de Processo.

Para a avaliação dos atributos de processos, são definidos critérios de avaliação que utilizam evidências, classificadas em dois grupos: práticas e produtos de trabalho. Essas evidências são a materialização da existência do critério avaliado. A seguir é exibido um quadro com a quantidade de critérios alcançados e não alcançados na avaliação de acordo com sua classificação e atributo de processo.

Tabela 23: Quantidade de critérios cumpridos por tipo de evidência, atributo de processo e nível de maturidade

Nível de Maturidade	Atributo de Processo	Evidencia	Sim	Não	Total
Nível 1- Executado	PA 1.1 - Execução do processo	Prática Base	8	1	9
		Produto de Trabalho	11	3	14
Nível 2 - Gerenciado	PA 2.1 - Gerência de execução	Prática Base	6	-	6
		Produto de Trabalho	6	4	10
	PA 2.2 - Gerência de produto de trabalho	Prática Base	4	-	4
		Produto de Trabalho	-	5	5
Nível 3 - Estabelecido	PA 3.1 - Definição de processo	Prática Base	4	1	5
		Produto de Trabalho	-	6	6
	PA 3.2 - Implementação de processo	Prática Base	6	-	6
		Produto de Trabalho	1	6	7
Nível 4 - Previsível	PA 4.1 - Medição de processo	Prática Base	4	2	6
		Produto de Trabalho	3	4	7
	PA 4.2 - Controle de processo	Prática Base	-	5	5
		Produto de Trabalho	-	6	6
Nível 5 - Em otimização	PA 5.1 - Inovação de processo	Prática Base	3	2	5
		Produto de Trabalho	-	5	5
	PA 5.2 - Otimização de processo	Prática Base	1	2	3
		Produto de Trabalho	-	3	3
Total			**57**	**55**	**112**

Na tabela 23 é possível observar que a partir do atributo de processo 2.2 nem todos os produtos de trabalho exigidos para demonstrar o alcance do objetivo do atributo de processo foram atendidos. Nos atributos de processo 2.2, 3.1, 4.2, 5.1 e 5.2 nenhum produto de trabalho foi apresentado como evidencia.

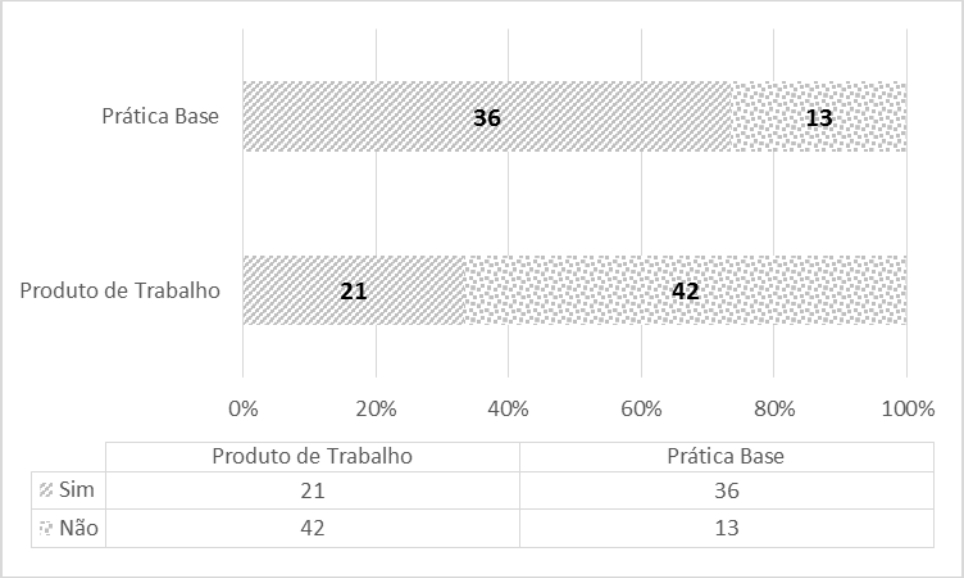


Figura 30: Distribuição dos critérios atendidos e não atendidos por tipo de evidência

É possível observar na figura 30 que a instituição executa um número elevado de práticas recomendadas para o processo de gestão de riscos de TI (73,5%), porém o cenário é inverso ao analisar os produtos de trabalho, onde apenas 1/3 dos produtos de trabalho estão implementados (33,3%).

4.6.2.1. Plano de ação

Conforme pôde ser visto nos resultados obtidos pela aplicação do instrumento de maturidade no item 4.6.2, a Coordenação de Gestão de Tecnologia da Informação da Fiocruz (CGTI) se encontra no nível 1 de maturidade (figura 27). O nível de 1 de maturidade é composto pelo atributo de processo 1.1, referente à execução do processo. Este atributo teve seus critérios amplamente alcançados (figura 28), onde apenas uma prática base e três produtos de trabalho não foram executados (tabela 23).

A figura 29 demonstra que o atributo de processo 1.1, referente ao nível 1 de maturidade, está 83% implementado e os atributos 2.1 e 2.2, referentes ao nível 2 de maturidade, se encontram 75% e 44% implementados, respectivamente.

Para que a CGTI alcance o nível 2 de maturidade (gerenciado) é necessário que seja minimamente implementados obrigatoriamente todos os critérios do atributo de processo do nível 1 (PA 1.1) e ao menos um dos critérios do atributo de processo 2.2 (rerente ao nível 2 de maturidade), tendo em vista que o atributo de processo 2.1 já apresenta a quantidade mínima necessária para sua classificação. Os critérios de avaliação que ainda não foram implementados são listados a seguir:

Tabela 24: Plano de ação para evolução da maturidade

Nível de maturidade	**Atributo de processo**	**Critério**	**Tipo de evidência esperada**	**Tipo de exigência**
Nível 1 - Executado	PA 1.1 – Execução do processo	Aprovar e garantir fundos para os planos de ação de riscos	Prática base	Obrigatório
		Plano de gerenciamento de riscos de projeto	Produto de trabalho	
		Riscos dos fornecedores		
		Resultados de testes de contingência		
Nível 2 - Gerenciado	PA 2.1 – Gerência de Execução	*Não é necessário, pois o atributo já alcançou os requisitos mínimos.*		
	PA 2.2	Plano de qualidade deve fornecer detalhes dos critérios de qualidade e estrutura e conteúdo do produto de trabalho	Produto de trabalho	Optativo. Ao menos um critério deve ser implementado para se alcançar a quantidade mínima requerida
		Documentação do processo deve fornecer detalhes dos controles (matriz de controles)		
		Plano de qualidade deve fornecer detalhes do produto de trabalho, critérios de qualidade, documentação exigida e controle de mudanças		
		Registro de qualidade deve fornecer uma trilha de auditoria das revisões realizadas.		

4.7. Documentos para o registro do processo de gestão de riscos de TI

Para que a avaliação pudesse ser realizada, foram aceitos como evidência artefatos que possuíssem conteúdos semelhantes aos produtos de trabalho esperados, independentemente de seus títulos. Assim, para que as próximas avaliações possam ser realizadas com base nos produtos de trabalho definidos na avaliação, está sendo sugerido um conjunto de documentos para o registro de todas as informações referentes ao processo de gestão de riscos de TI na unidade/órgão. Ao todo são nove documentos onde seus *templates*, cujos títulos e conteúdos estão aderentes ao modelo de referência do processo do COBIT, são apresentados a seguir.

1. Documentação do processo

1.1. Nome do processo

1.2. Dono do processo

A pessoa responsável pelo desenho do processo. Isto inclui a responsabilidade pela criação, atualização e aprovação de documentos (procedimentos, instruções/protocolos de trabalho) para suportar o processo.

1.3. Escopo do processo

Uma declaração clara de onde o processo começa e termina.

1.4. Regras do processo

Detalhes dos papéis chaves no processo:

- *Fornecedores e Entradas*
- *Saídas e Clientes*

1.5. Mapa de processos

Em geral, sob a forma de uma figura esquemática de um processo para mostrar o fluxo de trabalho sequencial. Na maior parte dos casos, haverá um mapa que mostra os fluxos através de um número de processos.

1.6. Matriz RACI

Identifica os principais atores do processo e suas responsabilidades, tais como, o responsável pela execução, dono do processo, quem deve ser consultado e quem deve ser informado.

1.7. Procedimentos do processo

Documento que descreve as atividades requeridas para o alcance dos resultados do processo.

2. Plano do processo

2.1. Objetivos de performance do processo

Varia de acordo com o projeto. No entanto, deve haver evidencias como metas, atividades necessárias, volumes de produção estimado, etc.

2.2. Recursos do processo

Um plano indicando recursos e informações necessárias para atender o desempenho requerido para o processo e informações sobre recursos que devem ser fornecidos.

2.3. Comunicação do processo

Um plano para comunicação requerida para o processo. Deve incluir informações como: responsabilidade pela comunicação, público alvo, conteúdo a ser comunicado, momento para a comunicação, etc.

2.4. Infraestrutura e ambiente de trabalho do processo

Instalações, ferramentas, métodos e ambiente de trabalho para a execução dos processos.

2.5. Competências exigidas para execução do processo

As descrições de trabalho e as habilidades necessárias para realizar o processo.

2.6. Formação exigida para o processo

Habilidades e competências dos usuários, incluindo os requisitos de formação individual.

3. Plano de qualidade

3.1. Declaração de política e objetivos de qualidade

Uma declaração de expectativas do cliente para o processo (ex. entregas ou pontualidade).

3.2. Conteúdo dos produtos de trabalho

Identificação de todos os produtos de trabalho, suas estruturas e conteúdos esperados.

3.3. Critérios de qualidade para os produtos de trabalho

Critérios pelos quais cada produto de trabalho será revisado e aprovado.

3.4. Documentação dos produtos de trabalho

Os requisitos para documentação e exigências de controle, incluindo identificação, rastreabilidade e aprovações.

3.5. Controle de mudanças de produtos de trabalho, versionamento e requisitos para gestão de configuração

Esboço para procedimentos de versionamento e controle de alterações aplicadas a produtos de trabalho.

4. Registro da qualidade

4.1. Registros dos comentários sobre requisitos e as medidas tomadas durante os controles e verificações de qualidade

Registros de comentários sobre questões relativas aos problemas encontrados em produtos de trabalho e resolução.

5. Políticas e normas

5.1. Objetivos organizacionais e responsabilidade pelo processo.

Uma declaração de objetivos da organização para o processo, uma vez que é aplicado em todas as unidades organizacionais. Deve identificar responsabilidades do processo.

5.2. Padrão mínimo de desempenho exigido para um processo

O nível de desempenho esperado para o processo em toda a organização. Isto pode incluir metas, atividades necessárias, volumes de produção estimado ou prazos.

5.3. Mapeamento de processos padrão, incluindo seu sequenciamento e interação

Um diagrama esquemático do fluxo de trabalho sequencial esperado para o processo e suas interações entre diferentes implementações do processo.

5.4. Procedimentos normalizados

Um documento que descreve os procedimentos que devem ser seguidos em todas as implementações dos processos.

5.5. Funções e competência para realizar o processo em padrões mínimos de desempenho

Descrições de trabalho padronizados e competências necessárias para o processo.

5.6. Infraestrutura (instalações, ferramentas, métodos, etc.) e ambiente de trabalho

As instalações, ferramentas, métodos e ambiente de trabalho necessários para a execução dos processos.

5.7. Relatórios e requisitos de monitoramento, incluindo auditoria e revisão

Relatórios esperados e requisitos de monitoramento para o processo, incluindo os requisitos de relatórios padronizado.

6. Plano de melhoria de desempenho

6.1. Objetivos de melhoria de processo

O nível de desempenho esperado do processo, com base em objetivos de negócios.

6.2. Análise das melhores práticas

Oportunidades para melhorias de processo identificadas com base na análise de comparação com as melhores práticas de mercado.

6.3. Oportunidades de melhoria da tecnologia

Oportunidades para melhorias do processo identificadas com base em análises de inovações de tecnologias e processos.

6.4. Ações de melhoria

Ações identificadas para melhorar o processo em toda a organização.

6.5. Plano de implementação de Melhoria

As melhorias propostas, ações planejadas para implementar essas melhorias, responsabilidades e prazo.

6.6. Abordagem da qualidade do projeto

Processo proposto para confirmar a realização das melhorias – métricas, comentários, etc.

7. Plano de métricas do processo

7.1. Objetivos de medição

Objetivos quantitativos em relação à qualidade e desempenho do processo, com base nas necessidades do cliente e objetivos de negócio.

7.2. Métricas / indicadores propostos

Identificação do que deve ser medido e seus indicadores.

7.3. Procedimento de coleta de dados

Definição de quais dados serão coletados para suportar a medição.

7.4. Procedimentos de análise

Identificação dos procedimentos de análise a serem utilizados, desde um gráfico simples até o mais sofisticado para análises quantitativas, como o controle de processo estatístico, modelagem estrutural ou outros métodos estatísticos multivariados.

8. Plano de controle do processo

8.1. Técnicas de controle

Uma descrição dos métodos utilizados para minimizar a variação de processo e produto. Isto irá diferir em cada processo e pode usar artefatos como normas, testes, revisões, passo a passo e teste.

8.2. Método de medição

Como a variação em cada processo será medida.

8.3. Limites de controle para o desempenho normal

Definição dos níveis aceitáveis de variação do processo.

9. Registro de desempenho do processo

9.1. Registro de revisões

Registro de desempenho atual do processo, com variações dos resultados esperados e ações tomadas para corrigir essas variações.

4.8. Conclusão

Este trabalho de pesquisa promoveu um estudo comparativo inédito entre os principais modelos de maturidade existentes no mercado e que produziu como resultado uma matriz comparativa que descreve de forma sistemática e objetiva suas principais características. A partir da matriz comparativa desenvolvida é possível obter de forma sintética as principais características dos modelos estudados, permitindo seu uso em futuras pesquisas sobre o tema ou ainda por organizações que queiram um panorama sobre as principais diferenças entre eles.

Outro resultado alcançado foi a seleção de um modelo de maturidade para avaliação da gestão de riscos de TI. Para isso, um grupo de especialistas no tema sugeriu de forma consensual um conjunto de critérios para a seleção do modelo. Esses critérios foram submetidos à opinião de gestores da instituição, que através da técnica de decisão multicritério AHP (*Analytic Hierarchy Process*) indicou o modelo de maturidade do COBIT 4.1 como o modelo mais adequado à instituição.

O desenvolvimento do trabalho apresentou um novo método para aplicação da técnica AHP, onde os objetos comparados não foram explicitamente declarados, mas substituídos por suas características. Isto 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 traduzidos em 112 novos critérios baseados em práticas e produtos de trabalho esperados, permitindo assim uma avaliação mais detalhada, com respostas menos subjetivas e com maior precisão na avaliação dos atributos de processo, sempre mantendo o alinhamento com os critérios originais.

A partir do instrumento desenvolvido e do modelo de referência do COBIT, foram especificados, com base na Metodologia de Desenvolvimento de Sistemas da Fiocruz, os requisitos para a definição de um sistema computacional para apoio à coleta de dados e avaliação da maturidade em gestão de riscos de TI. Isto permitirá que no futuro um sistema computacional para apoio ao processo de avaliação de maturidade possa ser desenvolvido.

Um protótipo do instrumento de avaliação proposto foi construído em Excel e aplicado na Coordenação de Gestão de Tecnologia da Informação – CGTI

da Fundação Oswaldo Cruz. A avaliação da CGTI demonstrou que é viável a utilização do instrumento e que os requisitos estão corretamente definidos. Foi possível identificar que a CGTI se encontra no nível 1 de maturidade (Executado), ou seja, que o processo de gestão de riscos atinge o seu propósito. O uso do protótipo do instrumento de avaliação evidenciou os *gaps* existentes e permitirá a CGTI esboçar um plano de ação para melhoria do seu processo de gestão de riscos de TI.

De forma complementar foi sugerido um conjunto de nove documentos que registram desde informações básicas sobre o processo de gestão de riscos de TI (nome, responsável, escopo, etc.) até questões sobre sua melhoria (plano de métricas, plano de desempenho, etc.). Desta forma, sugere-se que a organização passe a adotar esse conjunto de documentos a fim de registrar formalmente informações sobre seu processo de gestão de riscos e facilitar a demonstração de evidências (referentes aos produtos de trabalho) esperadas em avaliações futuras de maturidade em gestão de riscos de TI segundo o instrumento desenvolvido.

Espera-se que o trabalho realizado induza o desenvolvimento de trabalhos futuros para ampliação da pesquisa e desenvolvimento de novos artefatos. A pesquisa para escolha do modelo de maturidade poderá ser ampliada a partir da inclusão dos critérios que não puderam ser contemplados neste trabalho devido as restrições de prazo para sua conclusão. Um sistema computacional para suporte ao processo de avaliação de maturidade em gestão de riscos de TI também poderá ser construído com base nos requisitos especificados neste trabalho.

Outro trabalho que poderá ser desenvolvido é a avaliação em nível institucional, onde todas as áreas de TI da Fiocruz que desenvolvem atividades de gestão de riscos possam ser avaliadas, permitindo traçar um perfil institucional da maturidade em gestão de riscos de TI, subsidiando adequadamente à CGTI de informações para a proposição de políticas institucionais sobre o tema.

Outra aplicação possível é o uso da solução apresentada para avaliação de maturidade em outros órgãos da administração pública federal 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 organizações.

De uma forma geral, a solução proposta para avalição do nível de maturidade do processo de gestão de riscos de TI permitiu, além de identificar o nível atual de maturidade da CGTI, fornecer mecanismo para que a instituição evolua em seu processo de governança de TI, através do monitoramento e análise crítica em busca da melhoria contínua de seu processo de gestão de riscos.

Referências

ABNT – ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ISO 73. Primeira edição. *Gestão de riscos - Vocabulário*. Rio de Janeiro: ABNT, 2009a. 12 páginas.

_____. NBR ISO 15504-1:2008. Primeira edição. *Tecnologia da informação – Avaliação de processo*. Parte 1: Conceitos e vocabulário. Rio de Janeiro: ABNT, 2008a. 19 páginas.

_____. NBR ISO 15504-2:2008. Primeira edição. *Tecnologia da informação – Avaliação de processo*. Parte 2: Realização de uma avaliação. Rio de Janeiro: ABNT, 2008b. 16 páginas.

_____. NBR ISO 15504-4:2008. Primeira edição. *Tecnologia da informação – Avaliação de processo*. Parte 4: Orientação no uso para melhoria do processo e determinação da potencialidade do processo. Rio de Janeiro: ABNT, 2008c. 33 páginas.

_____. NBR ISO 15504-7:2009. Primeira edição. *Tecnologia da informação – Avaliação de processo*. Parte 7: Avaliação de maturidade de uma organização. Rio de Janeiro: ABNT, 2009b. 36 páginas.

_____. NBR ISO 31000:2009. Primeira edição. *Gestão de riscos – Princípios e diretrizes*. Rio de Janeiro: ABNT, 2009c. 24 páginas.

_____. NBR ISO 31010:2012. Primeira edição. *Gestão de riscos – Técnicas para o processo de avaliação de riscos*. Rio de Janeiro: ABNT, 2012. 96 páginas.

_____. NBR ISO/IEC 38500:2008. Primeira edição. *Governança corporativa de tecnologia da informação*. Rio de Janeiro: ABNT, 2008d. 15 páginas.

BERTALANFFY, Ludwig von. *Teoria Geral dos Sistemas – Fundamentos, desenvolvimento e aplicações*. Editora Vozes. Edição 3, 2008.

BHUSHAN, Navneet; RAI, Kanwal. *Strategic Decision Making: Applying the Analytic Hierarchy Process*. London, Springer: 2004.

BLATTNER, Peter. CIORCIARI, Maria. *Enterprise Risk Managemet Maturity* – Level Assessment Tool. Society of Actuaries. 2008.

BOULTON, Richard E. S.; LIBERT, Barry D.; SAMEK, Steve M. *Cracking the Value Code*: How successful businesses are creating wealth in the New Economy. New York, 2000.

BRASIL. Lei 12.527/2011. *Lei de acesso a informações*. Disponível em < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm> Acesso em 19/6/2013.

BRITO, Thiago D. *Levantamento e diagnóstico de maturidade da governança da segurança de informação na administração direta federal brasileira*. Brasília, 2011. Dissertação (Gestão do conhecimento e da tecnologia da informação). Universidade Católica de Brasília.

BRYMAN, Alan. *Research methods and organization studies*. London: Unwin Hyman, London, 1989.

BURGMAN, Rolando J.; HARRIS, Jeanne G. *Chains, Shops, and Networks*: The Logic of Organizational Value. 2005.

CARALLI, Rich. *Maturity Models in a Operational Context*. Software Engineering Institute. Carnegie Mellon. 2011.

CETIC – Centro de Estudos sobre as Tecnologias de Informação e da Comunicação. *Pesquisa sobre o uso das tecnologias da informação e da comunicação no Brasil* – TIC Domicílios e empresas 2011. São Paulo, 2012. Disponível em <http://op.ceptro.br/cgi-bin/cetic/tic-domicilios-e-empresas-2011.pdf >. Acesso em 10/10/2012.

_____. *Pesquisa sobre o uso das tecnologias da informação e da comunicação no Brasil* – TIC Governo Eletrônico 2010. São Paulo, 2010.Disponível em <http://op.ceptro.br/cgi-bin/cetic/tic-governo-2010.pdf> Acesso em 10/10/2012.

CHECKLAND, Peter. *Systems Thinking, Systems Practice*: includes a 30-year retrospective. John Wiley & Sons. New York, 1999.

CMMI Institute. *Catalog of Instructor Led CMMI Courses*. Disponível em < http://cmmiinstitute.com/training/>. Acesso em 5/11/2013.

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

CRAWFORD, J. Kent. *Project Management Maturity Model*. 2nd Edition. Auerbach Publications – Taylor & Francis Group. New York, 2007.

CTIR – Centro de Tratamento de Incidentes de Segurança de Rede de Computadores da Administração Pública Federal. *Estatísticas de Incidentes de Rede na APF* – 1º Trimestre/2013. Disponível em <http://www.ctir.gov.br/arquivos/estatisticas/2013/Estatisticas_CTIR_Gov_1o_Trimestre_2013.pdf> Acesso em 20/6/2013.

CURTIS, Patchin; CAREY, Mark. *Risk Assessment in Practice*. 2012.

DIONNE, Georges. *Risk Management*: history, definition and critique. Montreal, Canada Research Chair is Risk Management, HEC Montreal, 2013;

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 – GRSIC*. DSIC/ 2013. Disponível em <http://dsic.planalto.gov.br/documentos/nc_04_grsic.pdf>. Acesso em 12/5/2013.

ELMAALLAM, Mina, KRIOUILE, Abdelaziz. *Towards a model of maturity for is risk management*. International Journal of Computer Science & Information Technology, vol. 3, No 4, August, 2011.

FIOCRUZ – Fundação Oswaldo Cruz. *Auto Avaliação Fiocruz – Ciclo 2013*. Relatório de Gestão. Vice-Presidência de Gestão e Desenvolvimento Institucional. Fiocruz, 2013.

_____. *Diretoria Executiva*. Disponível em <http://portal.fiocruz.br/pt-br/content/diretoria-executiva>. Acesso em 4/1/2014.

_____. *Plano Quadrienal (2011-2014)*. Fiocruz/ 2011. Disponível em <http://www.fiocruz.br/media/planoquadrienal20112014.pdf> Acesso em 14/5/2013.

GSI – Gabinete de Segurança Institucional da Presidência da República. *Instrução Normativa GSI/PR nº 1/2008*. Gestão de Segurança da Informação e Comunicações na Administração Pública Federal. Disponível em <http://dsic.planalto.gov.br/documentos/in_01_gsidsic.pdf>. Acesso em Acesso em 12/5/2013.

HILL, Stephen. *Guia sobre a gestão de riscos no serviço público*. Brasília: Escola Nacional de Administração Pública, 2006. 58 p. (Cadernos ENAP, 30)

HILLSON, David A. *Towards a Risk Maturity Model. The International Journal of Project & Business Risk Management*. Vol I. No. I, Spring 1997, 35-45.

_____. *Organisational Maurity in Business Risk Management*: The IACCM Business Risk Management Maturity Model (BRM3). Version: 30th January 03 Version 014. 2002. Disponível em <http://www.risk-doctor.com/pdf-files/brm1202.pdf>. Acesso em 29/12/2013.

HOLANDA, Aurélio B. de In: *Novo Dicionário Eletrônico Aurélio*. versão 5.11. Edição 3. Positivo: 2004.

HOPKINSON, Martin. *Improving Risk Management Capability Using the Project Risk Maturity Model* - a Case Study Based on UK Defence Procurement Projects. PM World Today. Vol. XIII, Issue X. October 2011a.

_____. *The Project Risk Maturity Model*. Measuring and Improving Risk Management Capability. Gower. Burlington,VT, 2011b.

IBGC – Instituto Brasileiro de Governança Corporativa. *Código das melhores práticas da governança corporativa*. 4.ed. São Paulo, 2009.

_____. *Guia de Orientação para Gerenciamento de Riscos Corporativos*. São Paulo, SP: IBGC, 2007 (série de cadernos de governança corporativa, 3).

IIA – Institute of Internal Auditors. *Applying COSO's. Enterprise Risk Managemet* – Integrated Framework. September, 2004.

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

_____. *COBIT Self-assessment Guide*: Using COBIT 4.1. Illinois - USA, 2011b.

_____. *COBIT 5 for Information Security Introduction*. Illinois - USA, 2012a.

_____. *COBIT 5 - A Business Framework for the Governance and Management of Enterprise IT*. Illinois - USA, 2012b.

_____. _____. Implementation. Illinois - USA, 2012c.

ISO – International Organization for Standardization. *ISO 29148:2011. First Edition. Systems and software engineering* — Life cycle processes — Requirements engineering. Switzerland: ISO/IEC/IEEE, 2011. 83 páginas.

ITGI – IT Governance Institute. *COBIT 4.1*. Illinois - USA, 2007.

LAKATOS, Eva M.; MARCONI, Marina de A. *Metodologia do Trabalho Científico*. Edição 7. São Paulo, Atlas: 2011a.

_____. *Metodologia Científica*. Edição 6. São Paulo, Atlas: 2011b.

_____. *Técnicas de Pesquisa*. Edição 7. São Paulo, Atlas: 2012.

MPOG – Ministério do Planejamento, Orçamento e Gestão. *Guia de Orientação para o Gerenciamento de Riscos*. Versão 1.0 final. Disponível em <http://www.planejamento.gov.br/secretarias/upload/Arquivos/segep/brareino/acoes_do_projeto/gestao_de_risco-Oportunidade/produtos/130301_p_VII_risco_oportunidade.pdf> Acesso em 16/8/2013.

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 13/5/2013.

PROTIVITI. *Guide to Enterprise Risk Management*: Frequently Asked Questions. 2006.

_____. *Enterprise Risk Management*: Practical Implementation Advice. 2006. Volume 2, issue 6.

PWC – PricewaterhouseCoopers. *9ª Pesquisa de Líderes Empresariais Brasileiros*. Lidando com a adversidade. Relatório final. Março, 2013.

RAMOS, Anderson et al. *Security Officer*. Guia Oficial para Formação de Gestores de Segurança da Informação.Vol I. Edição 2. Zouk. Porto Alegre, 2008.

REHFELDT, Gládis K., *Monografia e Tese*: Guia Prático. Porto Alegre: Sulina, 1980.

ROSNAY, Joël de. *The Macroscope*. New York: Harper & Row, 1977 <Disponível em: http://pespmc1.vub.ac.be/macrbook.html> Acesso em 17/4/2013.

SAATY, Thomas L. *Theory and Applications of the Analytic Network Process*: Decision Making with Benefits, Opportunities, Costs, and Risks. Pittsburgh: RWS Publications, 2005.

_____. *Extending the Measurement of Tangibles to Intangibles*. International Journal of Information Technology & Decision Making, Vol. 8, No. 1, pp. 7-27, 2009.

SAATY, Thomas L.; VARGAS, Luis G. *Decision Making with the Analytic Network Process*: Economic, Political, Social and Technological Applications with Benefits, Opportunities, Costs and Risks. New York, Springer: 2006.

SANTOS NETO, Norival F. dos S. *Gerenciamento de Riscos dos Projetos*: uma proposta de modelo de maturidade. São Paulo, 2007, Tese (Engenharia Mecânica). Universidade Estadual de Campinas.

SEI – Software Engineering Institute. *CMMI for Services*. Version 1.3. Pittsburgh, PA. Carnegie Mellon. November, 2010.

_____. *Standard CMMI Appraisal Method for Process Improvement (SCAMPI) A*, Version 1.3: Method Definition Document. Pittsburgh, PA. Carnegie Mellon. March, 2011.

SHAHZAD, Basit; SAFVI, Sara Afzal. *Risk mitigation and management scheme based on risk priority*. Global Journal of Computer Science and Technology. Vol. 10 Issue 4 Ver. 1.0. p. 108-113, 2010.

SILVA, João M. da, *Apostila de Formação de valor em sistemas de atividades humanas*. Brasília, Faculdade de Tecnologia, Núcleo de Engenharia de Produção, UnB, 2012;

SILVEIRA, Alexandre Di Miceli da. *Governança Corporativa no Brasil e no Mundo*. Teoria e Prática. Rio de Janeiro: Elsevier, 2010.

SISP. *Estratégia Geral de Tecnologia da Informação (2013-2015)*. Disponível em <http://www.governoeletronico.gov.br/sisp-conteudo/estrategia-geral-de-ti/biblioteca/arquivos/estrategia-geral-de-tecnologia-da-informacao-trienio-2013-2015-v1_1> Acesso em 13/5/2013.

TCU. *Relatório do Levantamento Governança de TI 2010*. Disponível em <http://portal2.tcu.gov.br/portal/page/portal/TCU/comunidades/tecnologia_inf

ormacao/pesquisas_governanca/Relat%C3%B3rio%20do%20Levantamento%20Governan%C3%A7a%20de%20TI%202010.pdf>. Acesso em 12/5/2013.

_____. *Acórdão nº 1.603/2008-TCU-Plenário*. Disponível em <https://contas.tcu.gov.br/juris/Web/Juris/ConsultarTextual2/Jurisprudencia.faces?colegiado=PLENARIO&numeroAcordao=1603&anoAcordao=2008>. Acesso em 12/5/2013.

TM – TREND MICRO. Brasil. *Desafios de Segurança Cibernética Enfrentados por uma Economia em Rápido Crescimento*. 2013.

TRIANTAPHYLLOU, Evangelos. *Using the Analytic Hierarchy Process for Decision Making in Engineering Applications*: some chalelenges. Inter'l Journal of Industrial Engineering: Applications and Practice, Vol. 2, No. 1, pp. 35-44, 1995.

VARGAS, Ricardo 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 28/6/2013.

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

Anexos

Anexo A: Guia de entrevista/questionário

Exemplo de guia de entrevista/questionário utilizado para identificação de critérios para a avaliação de modelos de maturidade em gestão de riscos.

UNIVERSIDADE DE BRASÍLIA – UNB
MESTRADO EM COMPUTAÇÃO APLICADA - PPCA
DEPARTAMENTO DE CIÊNCIA DA COMPUTAÇÃO – CIC
DEPARTAMENTO DE ENGENHARIA DE PRODUÇÃO – EPR

Estudo comparativo de modelos de maturidade aplicados à gestão de riscos: uma abordagem sob a perspectiva da tecnologia da informação

Aluno: Misael Araújo - Orientador: Dr. Edgard Costa

Guia para entrevista / Questionário sobre características relevantes aos modelos de maturidade em gestão de riscos

Contextualização: entendendo a importância da gestão de riscos para o alcance dos objetivos estratégicos de uma organização e a importância da avaliação de maturidade como forma de melhoria da capacidade da organização no processo de gestão de riscos, pedimos sua contribuição no sentido de fornecer sua opinião sobre a questão abaixo.

Questão base: Quais são suas expectativas em relação a um modelo de maturidade em gestão de riscos, ou seja, quais características você considera importante ao escolher um modelo de maturidade de gestão de riscos com foco em TI?

Comentários:

Anexo B: Formulário para coleta de dados sobre preferência dos gestores da Fiocruz em relação aos modelos de maturidade em gestão de riscos

O formulário abaixo foi utilizado para a coleta de dados durante entrevista realizada com gestores da instituição sobre suas preferências em relação aos diferentes critérios dos modelos de maturidade. Os dados coletados foram posteriormente transferidos para a ferramenta *Expert Choice*, que apoiou a aplicação da técnica AHP para obtenção dos índices de cada um dos critérios.

Universidade de Brasília

UNIVERSIDADE DE BRASÍLIA – UNB
MESTRADO EM COMPUTAÇÃO APLICADA - PPCA
DEPARTAMENTO DE CIÊNCIA DA COMPUTAÇÃO – CIC
DEPARTAMENTO DE ENGENHARIA DE PRODUÇÃO – EPR

Estudo comparativo de modelos de maturidade aplicados à gestão de riscos: uma abordagem sob a perspectiva da tecnologia da informação

Aluno: Misael Araújo - Orientador: Dr. Edgard Costa

Formulário para coleta de dados sobre preferência dos gestores da Fiocruz em relação aos modelos de maturidade em gestão de riscos

Data:
Nome:
Função:

Critério: Quantidade de níveis de maturidade

Critério 1									Critério 2							
4 níveis									5 níveis							
9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9
Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério 1									Critério 2							
4 níveis									6 níveis							
9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9

Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério 1									Critério 2							
5 níveis									6 níveis							
9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9
Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério: Descrição das escalas de maturidade

Critério 1	Critério 2
Nível 1: Inicial	Nível 0: Incompleto
Nível 2: Gerenciado	Nível 1: Executado
Nível 3: Definido	Nível 2: Gerenciado
Nível 4: Gerenciado quantitativamente	Nível 3: Estabelecido
Nível 5: Otimizando	Nível 4: Previsível
	Nível 5: Em otimização

9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9
Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério 1	Critério 2
Nível 1: Inicial	Nível 1: Funcionamento
Nível 2: Gerenciado	Nível 2: Especialização
Nível 3: Definido	Nível 3: Crescimento
Nível 4: Gerenciado quantitativamente	Nível 4: Convergência
Nível 5: Otimizando	Nível 5: Referência

9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9
Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério 1	Critério 2
Nível 1: Inicial	Nível 1: Ingênuo
Nível 2: Gerenciado	Nível 2: Principiante
Nível 3: Definido	Nível 3: Normalizado
Nível 4: Gerenciado quantitativamente	Nível 4: Natural
Nível 5: Otimizando	

9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9
Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério 1	Critério 2
Nível 0: Incompleto Nível 1: Executado Nível 2: Gerenciado Nível 3: Estabelecido Nível 4: Previsível Nível 5: Em otimização	Nível 1: Funcionamento Nível 2: Especialização Nível 3: Crescimento Nível 4: Convergência Nível 5: Referência

9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9
Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério 1	Critério 2
Nível 0: Incompleto Nível 1: Executado Nível 2: Gerenciado Nível 3: Estabelecido Nível 4: Previsível Nível 5: Em otimização	Nível 1: Ingênuo Nível 2: Principiante Nível 3: Normalizado Nível 4: Natural

9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9
Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério 1	Critério 2
Nível 1: Funcionamento Nível 2: Especialização Nível 3: Crescimento Nível 4: Convergência Nível 5: Referência	Nível 1: Ingênuo Nível 2: Principiante Nível 3: Normalizado Nível 4: Natural

9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9
Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério: Dependência entre níveis

Critério 1	Critério 2

Sim									Não							
9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9
Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério: Estrutura

Critério 1									**Critério 2**							
Quantidade de níveis									Descrição das escalas de maturidade							
9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9
Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério 1									**Critério 2**							
Quantidade de níveis									Dependência entre níveis							
9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9
Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério 1									**Critério 2**							
Descrição das escalas de maturidade									Dependência entre níveis							
9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9
Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério: Domínio do modelo de referência

Critério 1									**Critério 2**							
Engenharia de software									Controle e Gerenciamento de TI							
9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9
Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério 1									**Critério 2**							
Engenharia de software									Genérico							
9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9

Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério 1									**Critério 2**							
Engenharia de software									. Gerenciamento de Risco							
9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9
Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério 1									**Critério 2**							
Controle e Gerenciamento de TI									Genérico							
9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9
Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério 1									**Critério 2**							
Controle e Gerenciamento de TI									Gerenciamento de Risco							
9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9
Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério 1									**Critério 2**							
Genérico									Gerenciamento de Risco							
9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9
Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério: Instrumentos de avaliação

Critério 1									**Critério 2**							
Oferece um conjunto de ferramentas com *templates* para o processo de avaliação.									Não oferece instrumentos, mas apresenta elementos para sua seleção, construção, etc.							
9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9

Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério: Entidade mantenedora

Critério 1								Critério 2								
SEI								ISACA								
9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9
Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério 1								Critério 2								
SEI								Acadêmico								
9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9
Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério 1								Critério 2								
SEI								ABNT/ISO								
9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9
Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério 1								Critério 2								
ISACA								Acadêmico								
9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9
Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério 1								Critério 2								
ISACA								ABNT/ISO								
9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9
Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério 1									Critério 2							
Acadêmico									ABNT/ISO							
9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9
Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério: Concepção

Critério 1									Critério 2							
Domínio do modelo de referência									Instrumentos de avaliação							
9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9
Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério 1									Critério 2							
Domínio do modelo de referência									Entidade mantenedora							
9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9
Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério 1									Critério 2							
Instrumentos de avaliação									Entidade mantenedora							
9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9
Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério: Alinhamento com outros documentos de referência

Critério 1									Critério 2							
CMM for SW, INCOSE SECAM e EIA 731 SECM (Engenharia de Software)									ITIL, ISO 17799, PMBOK, PRINCE2, VAL IT, ISO/IEC 15504-1, ISO/IEC 15504-2 (Serviços de TI, Gerência de Projetos, Governança de TI e Avaliação de Processos)							
9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9
Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério 1									Critério 2							
CMM for SW, INCOSE SECAM e EIA 731 SECM (Engenharia de Software)									ISO 9000, ISO/IEC 2382-1, ISO/IEC 2382-20, ISO/IEC 12207 e ISO/IEC 15288 (Qualidade, desenvolvimento de sistemas, engenharia de software, ciclo de vida de sistema)							
9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9
Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério 1									Critério 2							
ITIL, ISO 17799, PMBOK, PRINCE2, VAL IT, ISO/IEC 15504-1, ISO/IEC 15504-2 (Serviços de TI, Gerência de Projetos, Governança de TI e Avaliação de Processos)									ISO 9000, ISO/IEC 2382-1, ISO/IEC 2382-20, ISO/IEC 12207 e ISO/IEC 15288 (Qualidade, desenvolvimento de sistemas, engenharia de software, ciclo de vida de sistema)							
9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9
Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério: Tempo de mercado

Critério 1									Critério 2							
2 anos									5 anos							
9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9
Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério 1									Critério 2							
2 anos									6 anos							
9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9
Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério 1									Critério 2							
2 anos									7 anos							
9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9

Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério 1									Critério 2							
2 anos									16 anos							
9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9
Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério 1									Critério 2							
5 anos									6 anos							
9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9
Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério 1									Critério 2							
5 anos									7 anos							
9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9
Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério 1									Critério 2							
5 anos									16 anos							
9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9
Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério 1									Critério 2							
6 anos									7 anos							
9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9
Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério 1	Critério 2

6 anos									16 anos								
9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	
Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta	

Critério 1									**Critério 2**								
7 anos									16 anos								
9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	
Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta	

Critério: Robustez

Critério 1									**Critério 2**								
Alinhamento com outros documentos									Tempo de mercado								
9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	
Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta	

Critério: Rastreabilidade

Critério 1									**Critério 2**								
Sim									Não								
9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	
Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta	

Critério: Benchmarking

Critério 1									**Critério 2**								
Nativo									Depende de método externo								
9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	
Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta	

Critério: Customização

Critério 1	**Critério 2**
Sim	Não

9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9
Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério: Flexibilidade

Critério 1									**Critério 2**							
Rastreabilidade									Benchmarking							
9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9
Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério 1									**Critério 2**							
Rastreabilidade									Customização							
9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9
Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério 1									**Critério 2**							
Benchmarking									Customização							
9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9
Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério: Custo com capacitação

Critério 1									**Critério 2**							
Sem custo									R$ 1.080,00							
9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9
Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério 1									**Critério 2**							
Sem custo									R$ 1.291,29							
9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9

Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério 1								Critério 2								
Sem custo								R$ 7.043,40								
9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9
Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério 1								Critério 2								
R$ 1.080,00								R$ 1.291,29								
9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9
Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério 1								Critério 2								
R$ 1.080,00								R$ 7.043,40								
9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9
Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério 1								Critério 2								
R$ 1.291,29								R$ 7.043,40								
9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9
Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério: Custo com material de referência

Critério 1								Critério 2								
Sem custo								R$ 469,56								
9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9

Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério 1									**Critério 2**							
Sem custo									R$ 555,00							
9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9
Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério 1									**Critério 2**							
R$ 469,56									R$ 555,00							
9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9
Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério: Custos

Critério 1									**Critério 2**							
Custo com capacitação									Custo com material							
9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9
Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério: Critérios para escolha de um modelo

Critério 1									**Critério 2**							
Estrutura									Concepção							
9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9
Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério 1									**Critério 2**							
Estrutura									Robustez							
9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9

Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério 1									**Critério 2**							
Estrutura									Flexibilidade							
9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9
Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério 1									**Critério 2**							
Estrutura									Custos							
9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9
Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério 1									**Critério 2**							
Concepção									Robustez							
9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9
Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério 1									**Critério 2**							
Concepção									Flexibilidade							
9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9
Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério 1									**Critério 2**							
Concepção									Custos							
9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9
Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério 1	**Critério 2**

Robustez									Flexibilidade							
9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9
Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério 1									**Critério 2**							
Robustez									Custos							
9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9
Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Critério 1									**Critério 2**							
Flexibilidade									Custos							
9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9
Absoluta		Muito forte		Forte		Moderada		Igual		Moderada		Forte		Muito forte		Absoluta

Anexo C: Formulário para avaliação das entrevistas

O formulário a seguir foi utilizado para avaliação da percepção dos entrevistados em um pré-teste das entrevistas para medida de opinião.

Universidade de Brasília

UNIVERSIDADE DE BRASÍLIA – UNB
MESTRADO EM COMPUTAÇÃO APLICADA - PPCA
DEPARTAMENTO DE CIÊNCIA DA COMPUTAÇÃO – CIC
DEPARTAMENTO DE ENGENHARIA DE PRODUÇÃO – EPR

Estudo comparativo de modelos de maturidade aplicados à gestão de riscos: uma abordagem sob a perspectiva da tecnologia da informação

Aluno: Misael Araújo - Orientador: Dr. Edgard Costa

Formulário para avaliação da entrevista realizada

1) Em relação a entrevista realizada, por favor, indique a sua opinião em relação aos itens abaixo:

1. Clareza da proposta da entrevista				
○ Péssima	○ Ruim	○ Indiferente	○ Boa	○ Ótima
2. Habilidade do entrevistado em explicar conceitos, esclarecer dúvidas e conduzir a entrevista				
○ Péssima	○ Ruim	○ Indiferente	○ Boa	○ Ótima
3. Clareza do método AHP para comparação dos critérios				
○ Péssima	○ Ruim	○ Indiferente	○ Boa	○ Ótima
4. Compreensão dos critérios utilizados na avaliação				
○ Incompreensão absoluta	○ Incompreensão da maior parte	○ Indiferente	○ Compreensão da maior parte	○ Compreensão absoluta
5. Tempo despendido para participação da entrevista				
○ Excessivo	○ Inadequado	○ Indiferente	○ Adequado	○ Ideal

2) Outros comentários:

_____

_____

Anexo D: Resultados consolidados dos grupos de critérios avaliados

Abaixo estão descritos os resultados finais das avaliações dos gestores da instituição (combinação das respostas individuais), segundo a hierarquia de critérios determinada.

Critérios de nível 1

	Estrutura	Concepção	Robustez	Flexibilida	Custos
Estrutura		1,57042	1,11045	1,19279	4,06321
Concepção			2,37618	1,9786	3,92834
Robustez				1,20094	2,58734
Flexibilidade					2,90419
Custos	Incon: 0,01				

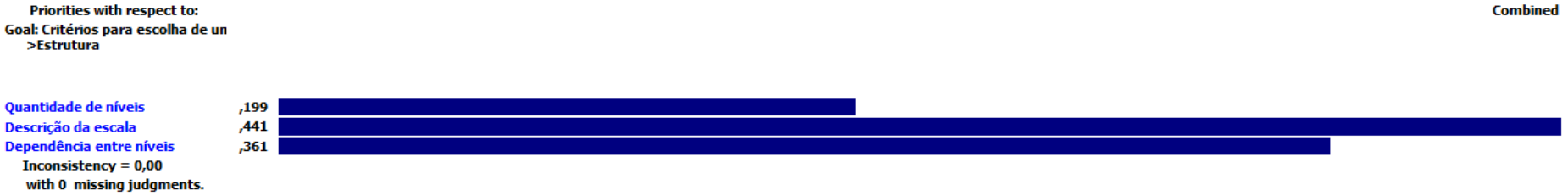
Priorities with respect to:
Goal: Critérios para escolha de ...

Combined

Inconsistency = 0,01
with 0 missing judgments.

Critério de nível 2: Estrutura

	Quantidade	Descrição	Dependênc
Quantidade de níveis		2,22091	1,80861
Descrição da escala			1,21901
Dependência entre níveis	Incon: 0,00		



Critério de nível 3: Estrutura/Quantidade de níveis

	4 níveis	5 níveis	6 níveis
4 níveis		1,48675	1,45785
5 níveis			1,14471
6 níveis	Incon: 0,00		

Critério de nível 3: Estrutura/Descrição da escala

	Inicial, Ger	Incompleto	Funcionam	Ingênuo, P
Inicial, Gerenciado, Definido, Gerenciado quantitativamente, Otimizado		1,15556	2,55966	5,53684
Incompleto, Executado, Gerenciado, Estabelecido, Previsível, Em otimização			1,77713	4,51799
Funcionamento, Especialização, Crescimento, Convergência, Referência				3,04683
Ingênuo, Principiante Normalizado, Natural	Incon: 0,00			

Critério de nível 3: Estrutura/Dependência entre níveis

	Sim	Não
Sim		3,60774
Não	Incon: 0,00	

Critério de nível 2: Concepção

	Domínio dc	Instrument	Entidade m
Domínio do modelo de referência		1,29271	1,99476
Instrumentos de avaliação			2,22091
Entidade mantenedora	Incon: 0,01		

Priorities with respect to:
Goal: Critérios para escolha de um m
>Concepção

Combined

Critério de nível 3: Concepção/Domínio do modelo de referência

	Engenharia	Controle e	Genérico	Gerenciam
Engenharia de SW		2,76823	1,44225	5,68054
Controle e Gerenciamento de TI			3,04683	2,15443
Genérico				3,94683
Gerenciamento de Risco	Incon: 0,01			

Priorities with respect to:
Goal: Critérios para escolha de um m
>Concepção
>Domínio do modelo de refer...

Combined

Critério de nível 3: Concepção/Instrumentos de avaliação

	Oferece um	Não oferec
Oferece um conunto de ferramentas com templates para o processo de avaliação.		5,92394
Não oferece instrumentos, mas apresenta elementos para sua seleção, construção, etc.	Incon: 0,00	

Priorities with respect to: Combined
Goal: Critérios para escolha de um mc
>Concepção
>Instrumentos de avaliação

Inconsistency = 0,00
with 0 missing judgments.

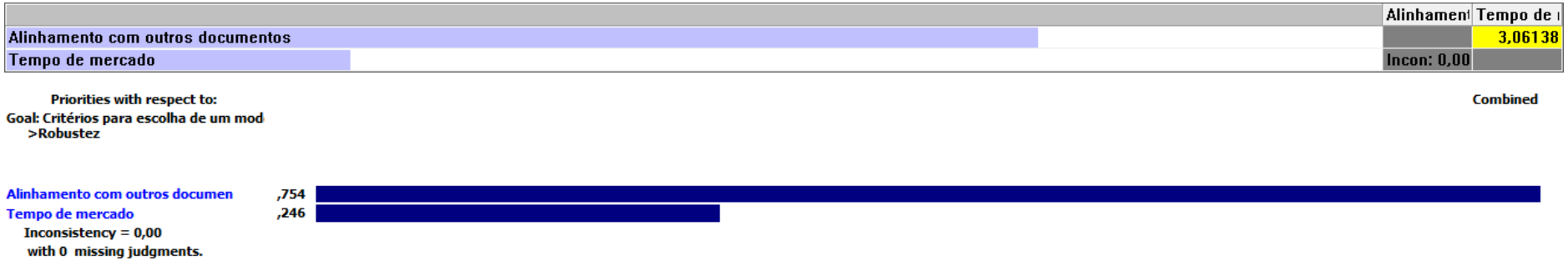
Critério de nível 3: Concepção/Entidade mantenedora

	SEI	ISACA	Acadêmico	ABNT/ISO
SEI		3,89653	1,3896	3,92834
ISACA			3,57852	1,66882
Acadêmico				5,23489
ABNT/ISO	Incon: 0,01			

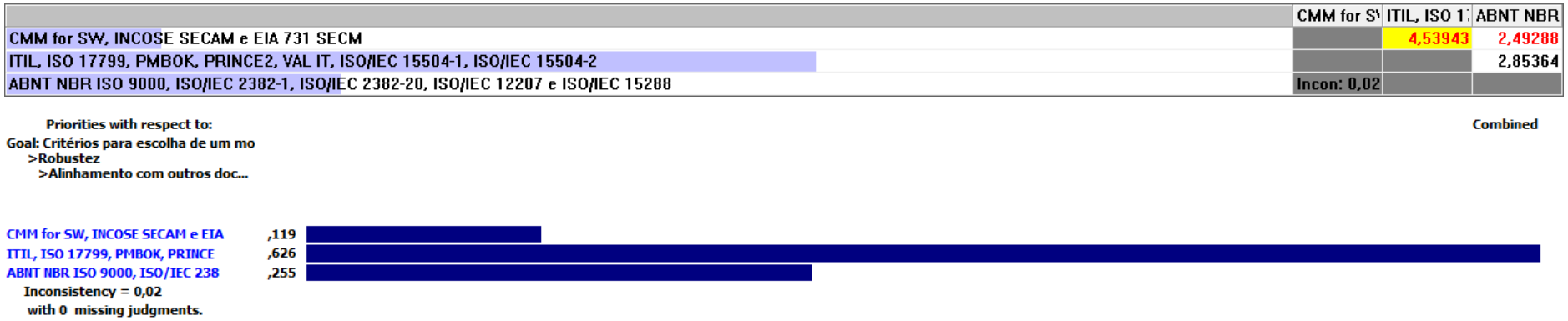
Priorities with respect to: Combined
Goal: Critérios para escolha de un
>Concepção
>Entidade mantenedora

Inconsistency = 0,01
with 0 missing judgments.

Critério de nível 2: Robustez



Critério de nível 3: Robustez/Alinhamento com outros documentos



Critério de nível 3: Robustez/Tempo de mercado

	2 anos	5 anos	6 anos	7 anos	16 anos
2 anos		3,36042	3,41995	2,22091	1,07642
5 anos			1,06991	1,22221	1,20659
6 anos				1,41421	1,37473
7 anos					1,31381
16 anos	Incon: 0,02				

Priorities with respect to:
Goal: Critérios para escolha de un
>Robustez
>Tempo de mercado

Combined

Inconsistency = 0,02
with 0 missing judgments.

Critério de nível 2: Flexibilidade

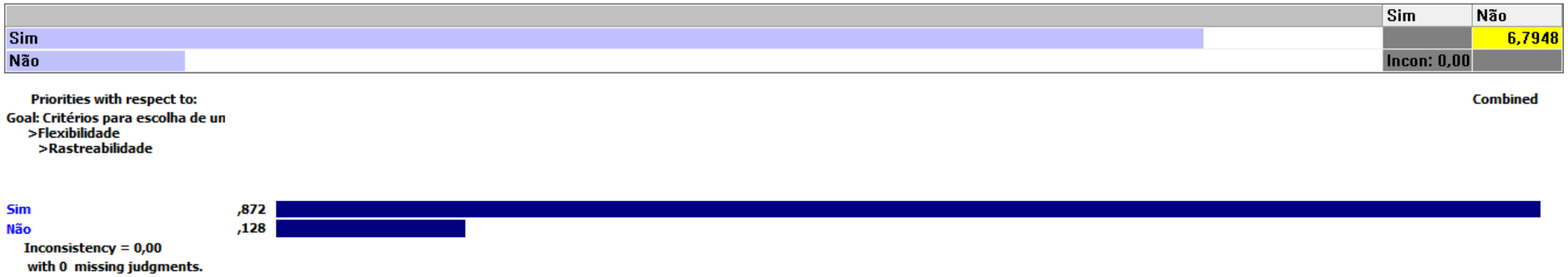
	Rastreabili	Benchmarl	Customiza
Rastreabilidade		2,79083	1,661
Benchmarking			1,20094
Customização	Incon: 0,01		

Priorities with respect to:
Goal: Critérios para escolha de un
>Flexibilidade

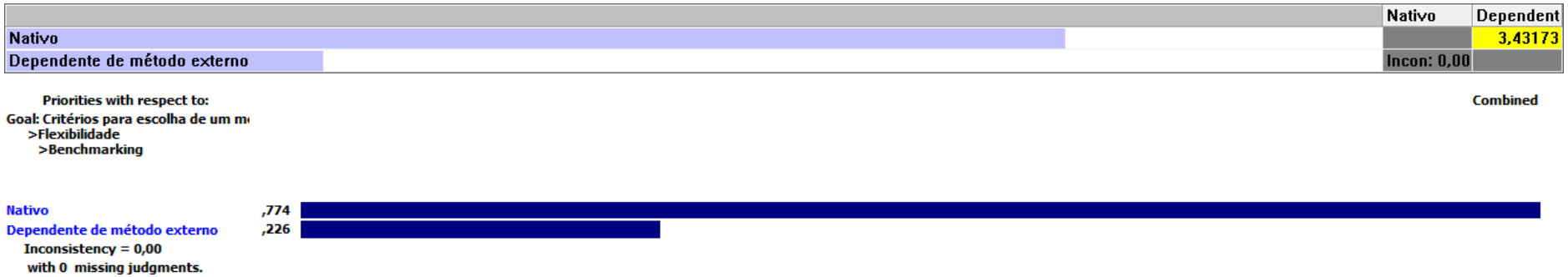
Combined

Inconsistency = 0,01
with 0 missing judgments.

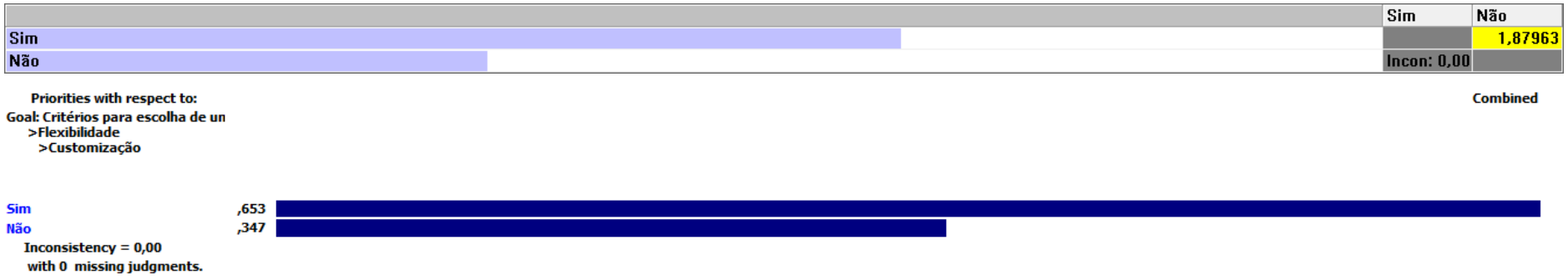
Critério de nível 3: Flexibilidade/Rastreabilidade



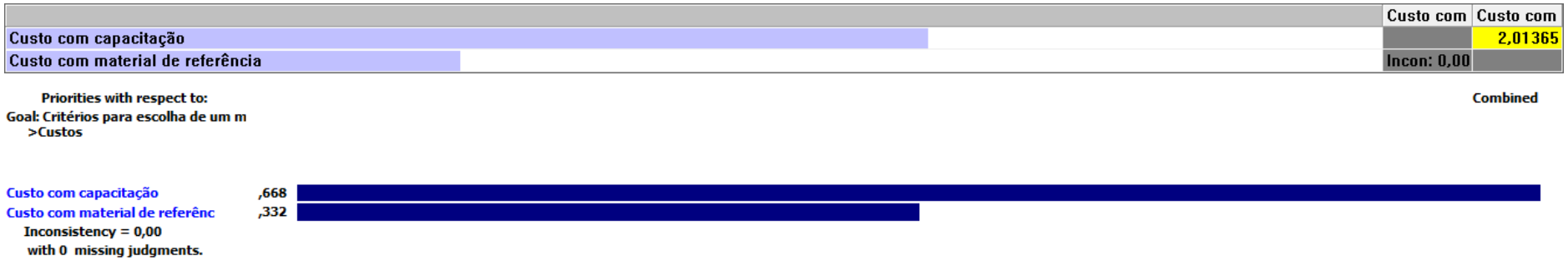
Critério de nível 3: Flexibilidade/Benchmarking



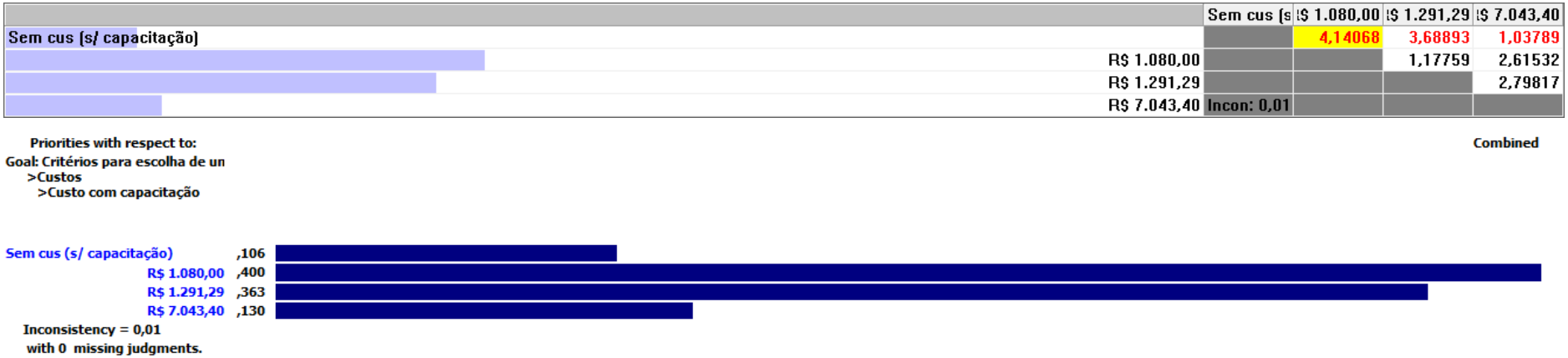
Critério de nível 3: Flexibilidade/Customização



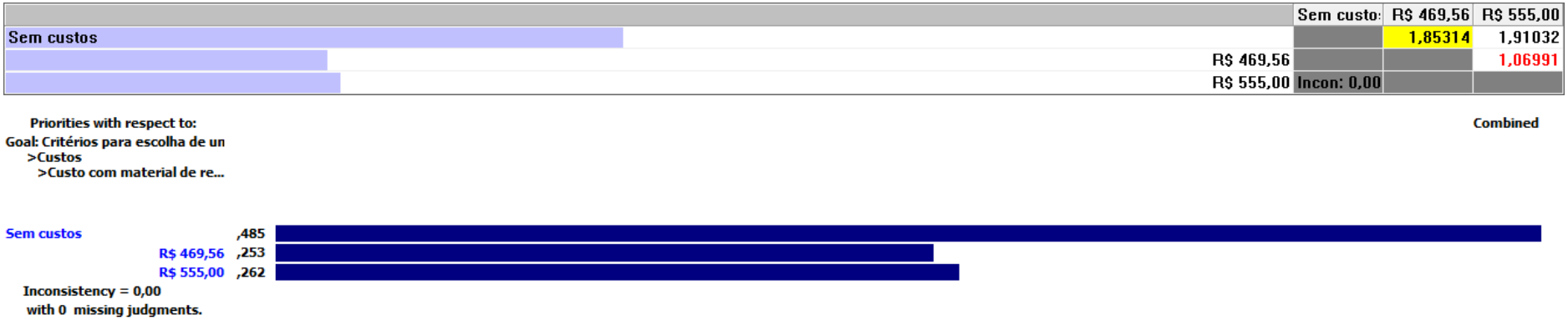
Critério de nível 2: Custos



Critério de nível 3: Custos/Custo com capacitação



Critério de nível 3: Custos/Custo com material de referência



Anexo E: Resultados da Avaliação do Processo (ISACA, 2011b)

A tabela abaixo é sugerida pelo guia de auto avaliação do COBIT para que a organização indique quais processos estão sendo avaliados, qual o nível alvo e qual o nível efetivamente alcançado.

Resultados da Avaliação do Processo								
Nome do processo	**Avaliado?**	**Nível alvo?**	**Nível de capacidade do processo**					
			0	**1**	**2**	**3**	**4**	**5**
Planejar e Organizar								
PO1 Definir um Plano Estratégico de TI								
P02 Definir a Arquitetura da Informação								
PO3 Determinar o Direcionamento Tecnológico								
PO4 Definir os Processos, Organização e os Relacionamentos de TI								
PO5 Gerenciar o Investimento de TI								
PO6 Comunicar as Diretrizes e Expectativas da Diretoria								
PO7 Gerenciar os Recursos Humanos de TI								
PO8 Gerenciar a Qualidade								
PO9 Avaliar e Gerenciar os Riscos de TI								
PO10 Gerenciar Projetos								
Adquirir e Implementar								
AI1 Identificar Solução Automatizadas								
AI2 Adquirir e Manter Software Aplicativo								
AI3 Adquirir e Manter Infraestrutura de Tecnologia								
AI4 Habilitar Operação e Uso								
AI5 Adquirir Recursos de TI								
AI6 Gerenciar Mudanças								
AI7 Instalar e Homologar Soluções e Mudanças								
Entregar e Suportar								
DS1 Definir e Gerenciar Níveis de Serviços								
DS2 Gerenciar Serviços de Terceiros								
DS3 Gerenciar Capacidade e Desempenho								
DS4 Assegurar Continuidade de Serviços								
DS5 Assegurar a Segurança dos Serviços								
DS6 Identificar e Alocar Custos								
DS7 Educar e Treinar os Usuários								
DS8 Gerenciar a Central de Serviço e os Incidentes								
DS9 Gerenciar a Configuração								
DS10 Gerenciar os Problemas								
DS11 Gerenciar os Dados								
DS12 Gerenciar o Ambiente Físico								
DS13 Gerenciar as Operações								
Monitorar e Avaliar								
ME1 Monitorar e Avaliar o Desempenho								

ME2 Monitorar e Avaliar os Controles Internos								
ME3 Assegurar a Conformidade com Requisitos Externos								
ME4 Prover a Governança de TI								

Fonte: ISACA (2011b)

Anexo F: Modelo de Auto Avaliação

O guia de auto avaliação do COBIT sugere ainda o uso das duas tabelas abaixo, onde a primeira é utilizada para o registro dos índices alcançados em cada um dos produtos de processo e o nível de capacidade alcançado. A segunda tabela apresenta o resultado detalhado das avaliações, indicado o nível alcançado pelos atributos de processo de acordo com o conjunto de critérios avaliados.

Seção 1: Resumo do resultado da avaliação

Nome do Processo	**Nível 0**	**Nível 1**	**Nível 2**		**Nível 3**		**Nível 4**		**Nível 5**	
		PA 1.1	PA 2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2	PA 5.1	PA 5.2
Avaliação por critério										
Nível de capacidade alcançado										
Legenda: **N** (Não atingido, 0 - 15%) **P** (Parcialmente atingido, > 15% - 50%) **L** (Amplamente atingido, > 50% - 85%) **F** (Completamente atingido, > 85% - 100%)										

Seção 2: Avaliação detalhada para o processo PO9

Nível	**Avaliar se os resultados a seguir são alcançados**	**Critério**	**Comentários**	**N (0-15%)**	**P (>15-50%)**	**L (>50-85%)**	**F (>85-100%)**
Nível 0 Incompleto	O processo não é implementado ou não consegue atingir seu objetivo.	Neste nível, há pouca ou nenhuma evidência de qualquer realização do propósito do processo.					
Nível 1 Executado	PA 1.1 Execução do processo – o propósito do processo é atingido	Os seguintes resultados do processo estão sendo alcançados: • P09-1 Uma estrutura de gestão de riscos está estabelecida e alinhada à estrutura de gestão de riscos da organização. • P09-2 Planos de ação para tratamento do risco são definidos e comunicados.					

Nível 2 Gerenciado	PA 2.1 Gerência de Execução – uma medida da extensão na qual a execução do processo é gerenciada	Como resultado do alcance completo deste atributo: a) Objetivos para a execução do processo são identificados; b) Execução do processo é planejada e monitorada; c) Execução do processo é ajustada para atender os planos; d) Responsabilidades e autoridades para execução do processo são definidas, atribuídas e comunicadas; e) Recursos e informações necessárias para a execução do processo são identificados, disponibilizados, alocados e utilizados; f) Interfaces entre as partes envolvidas são gerenciadas para garantir tanto a comunicação efetiva quanto a atribuição clara das responsabilidades;					
	PA 2.2 Gerência de produto de trabalho – uma medida da extensão na qual os produtos de trabalho são gerenciados apropriadamente. O produto de trabalho (ou saídas do processo) são definidos e controlados.	Como resultado do alcance completo deste atributo: a) Requisitos para produtos de trabalho do processo são definidos; b) Requisitos para a documentação e controle dos produtos de trabalho são definidos; c) Produtos de trabalho são identificados, documentados e controlados apropriadamente;					

		d) Produtos de trabalho são revisados de acordo com o planejado e ajustados, quando necessário, para atender os requisitos;					
Nível 3 Estabelecido	PA 3.1 Definição de processo – uma medida da extensão na qual um processo padrão é mantido para apoiar a implementação do processo definido.	Como resultado do alcance completo deste atributo: a) Um processo padrão, incluindo diretrizes apropriadas para sua adaptação, é definido para descrever os elementos fundamentais que devem ser incorporados num processo definido; b) A sequência e a interação do processo padrão com outros processos são determinadas; c) Competências e papéis requeridos para execução do processo são identificadas como parte do processo padrão; d) Infraestrutura e ambiente de trabalho requeridos para execução de um processo são identificados como parte do processo padrão; e) Métodos apropriados para monitorar a eficácia e adequação dos processos são determinados;					
	PA 3.2 Implementação do processo – uma medida de extensão na qual o processo padrão é efetivamente implementado como um processo definido para	Como resultado do alcance completo deste atributo: a) Um processo definido é implementado com base em um processo padrão apropriadamente					

	atingir seus resultados.	selecionado e/ou adaptado; b) Os papéis, autoridades e responsabilidades requeridos para execução do processo definido são atribuídos e comunicado; c) As pessoas que executam o processo definido são competentes em termos de educação, treinamento e experiência apropriados; d) Recursos e informações requeridos para a execução do processo definido são disponibilizados, alocados e utilizados; e) Infraestrutura e ambiente de trabalho requeridos para execução do processo definido são disponibilizados, gerenciados e mantidos; f) Dados apropriados são coletados e analisados, constituindo uma base para o entendimento do comportamento do processo, para demonstrar a adequação e eficácia do processo, e avaliar onde pode ser feita a melhoria contínua do processo.					
Nível 4 Previsível	PA 4.1 Medição de processo – uma medida que quantifica a utilização dos resultados de medições para garantir que a	Como resultado do alcance completo deste atributo: a) Necessidades de informação de processo são estabelecidas para apoiar o alcance de					

	execução do processo apoie o alcance de objetivos relevantes de desempenho para suportar o alcance das metas definidas para o negócio.	metas de negócio definidas e relevantes; b) Objetivos de medição de processo são derivados de necessidades de informação de processo; c) Objetivos quantitativos para o desempenho do processo são estabelecidos em apoio ao alcance de metas relevantes de negócio; d) Medidas e frequências de medição são identificadas e definidas de forma alinhada com os objetivos de medição de processo e os objetivos quantitativos para o desempenho do processo; e) Resultados da medição são coletados, analisados e comunicados para monitorar a extensão na qual os objetivos quantitativos para o desempenho do processo são alcançados; f) Resultados de medição são usados para caracterizar o desempenho do processo.					
	PA 4.2 Controle de processo – uma medida na qual o processo é gerenciado quantitativamente, resultando em um processo estável, capaz e previsível	Como resultado do alcance completo deste atributo: a) Técnicas de análise e controle são determinadas e aplicadas onde apropriado; b) Limites de controle de variação são					

	dentro de limites definidos.	estabelecidos para o desempenho normal do processo; c) Dados de medição são analisados para identificar causas especiais de variação; d) Ações corretivas são tomadas para tratar as causas especiais de variação; e) Limites de controle são restabelecidos (se necessário) seguindo a ação corretiva;					
Nível 5 Em otimização	PA 5.1 Inovação de processo – uma medida na qual as mudanças ocorridas no processo são identificadas através de análises das causas comuns de variação em sua execução e da investigação de abordagens inovadoras para a definição e implementação do processo.	Como resultado do alcance completo deste atributo: a) Objetivos de melhoria de processo são definidos para o processo em questão a fim de apoiar os objetivos de negócios relevantes; b) Dados apropriados são analisados para identificar as causas comuns das variações na execução do processo; c) Dados apropriados são analisados para identificar oportunidades para melhores práticas de inovação; d) Oportunidades de melhoria derivadas de novas tecnologias e novos conceitos de processo são identificadas; e) Uma estratégia é estabelecida visando atingir os objetivos de melhoria do processo.					
	PA 5.2 Otimização de processo – uma medida na qual as	Como resultado do alcance completo deste atributo:					

	mudanças na definição, gerenciamento e execução do processo resultam em um impacto eficaz, que atende aos objetivos relevantes de melhoria do processo.	a) O impacto de todas as mudanças propostas é avaliado em relação aos objetivos do processo definido e do processo padrão; b) A implementação de todas as mudanças acordadas é gerenciada para garantir que qualquer mau funcionamento da execução do processo seja compreendido e ações sejam tomadas; c) A eficácia da mudança do processo, com base na execução real, é avaliada com relação aos requisitos definidos para o produto e aos objetivos do processo, visando determinar se os resultados são devido a causas comuns ou especiais.					

Fonte: ISACA (2011b)