Revista Gestão & Tecnologia
e-ISSN: 2177-6652
revistagt@fpl.edu.br
http://revistagt.fpl.edu.br/

Estrutura Analítica de Riscos em Projetos de Desenvolvimento de *Software* no Setor Bancário: Um Estudo Exploratório

Risk Breakdown Structure on *Software* Development Projects in the Banking Sector: An Exploratory Study

Marco Alexandre Terlizzi
Mestrando em Gestão de Projetos pela Uninove, São Paulo, SP, Brasil
Pós-graduado em Administração pela FGV, São Paulo, SP, Brasil
alexandre.terlizzi@gmail.com

César Augusto Biancolino
Doutor em Controladoria e Contabilidade pela FEA/USP, São Paulo, SP, Brasil
Mestre em Controladoria e Contabilidade pela FECAP, São Paulo, SP, Brasil
Professor do Mestrado Profissional em Gestão de Projetos da Uninove, São Paulo, SP, Brasil
biancolino@gmail.com

Editor Científico: José Edson Lara
Organização Comitê Científico
Double Blind Review pelo SEER/OJS
Recebido em 18.01.2014
Aprovado em 09.04.2014

RESUMO

A gestão de riscos é uma área muito desenvolvida no setor bancário. Ao analisar os modelos de referência para a gestão de riscos da ISO (*International Organization for Standardization*), PMI (*Project Management Institute*) e SEI (*Software Engineering Institute*), observa-se que a identificação e categorização dos registros de riscos são imprescindíveis para a adequada gestão de riscos, pois os riscos somente são gerenciáveis quando identificados e documentados de forma clara e precisa. Foram selecionados 359 registros de riscos de dezesseis projetos de tecnologia de um banco brasileiro. Os riscos foram categorizados e agrupados segundo a taxonomia proposta pelo SEI para projetos de tecnologia e, após análise dos dados, foi possível identificar problemas na organização: (1) falta de clareza na especificação dos requisitos; (2) conflitos entre gestores de projetos e gestores funcionais; e (3) instabilidade no ambiente de teste integrado e homologação. Conclui-se que a adequada identificação e a categorização de riscos trazem benefícios à organização, pois permitem apresentar os problemas recorrentes em uma visão estratégica.

Palavras-chave: Gestão de Projetos; Gestão de Riscos; Identificação de Riscos; Estrutura Analítica de Riscos (EAR); ISO 31000.

ABSTRACT

Risk management is a very developed subject in the banking sector. This study analyzed reference models for risk management like ISO (*International Organization for Standardization*), PMI (*Project Management Institute*) and SEI (*Software Engineering Institute*), it was possible to observe that the identification and categorization of risks registers are essential for the appropriate risk management, because the risks are manageable only when identified and documented clearly and accurately. 359 risk records were selected from sixteen IT projects of a brazilian bank. Risks were categorized and grouped according to the taxonomy proposed by SEI and, after analyzing the data, it was possible to identify some problems in the organization: (1) lack of clarity in the requirements specification; (2) conflicts between project managers and functional managers; and (3) instability in the integrated test environment and homologation environment. It is possible to conclude that the proper identification and categorization of risks bring benefits to the organization because it allows presenting the recurrent problems in a strategic vision.

Keywords: Project Management; Risk Management; Risk Identification: Risk Breakdown Structure (RBS); ISO 31000.

1 INTRODUÇÃO

Segundo o PMI (2013), risco é um evento ou uma condição incerta que, se ocorrer, provocará um efeito positivo ou negativo nos objetivos do projeto tais como custo, escopo, prazo ou qualidade. A gestão dos riscos é uma área muito desenvolvida em instituições financeiras, principalmente em bancos e companhias seguradoras (Salles Jr., Soler, Valle, & Rabechini Jr., 2010). Para um banco, a análise de risco é um componente fundamental para garantir a competitividade e continuidade dos negócios. Por exemplo, para aprovar a concessão de um crédito para um cliente, o banco deve prever por meio de modelos matemáticos qual a real possibilidade de recebimento deste crédito e, para isto, utiliza-se de robustos sistemas computacionais que analisam o perfil do cliente em conjunto com dados históricos de variáveis mercadológicas.

Em 2012 o setor bancário brasileiro investiu R$20,1 bilhões em tecnologia, sendo R$ 8 bilhões em hardware, R$ 7,5 bilhões em software (crescimento de 23% em relação a 2011), R$ 4,2 bilhões em telecomunicações e R$ 400 milhões em outras tecnologias (Febraban, 2013). Estes números demonstram que nos próximos anos, para atender à crescente demanda de desenvolvimento de softwares, os bancos precisarão investir na contratação e/ou capacitação de talentos especializados na gestão de projetos de desenvolvimento de software e gestão de riscos.

Ao analisar os processos de três modelos de referência para a gestão de riscos desenvolvidos ao longo do tempo por renomadas instituições internacionais, observa-se que o processo de identificação de riscos é imprescindível em todos os modelos. Os modelos analisados foram: (1) *Software Risk Management* – é uma metodologia de gestão de riscos específica para projetos de desenvolvimento de software que foi proposta pelo SEI em 1996 e é amplamente utilizada nos dias atuais por empresas desenvolvedoras de software, principalmente por empresas com certificação CMMI nível 5 (Higuera & Haimes, 1996); (2) *ISO 31000* – é um modelo genérico para a gestão de riscos elaborado pela ISO em 2009 e oferece os princípios e diretrizes para gerenciar qualquer forma de riscos de uma maneira sistemática, transparente e confiável, dentro de qualquer escopo e contexto (ISO/ABNT, 2009); e (3) *PMBOK 5ª edição* – é um guia de boas práticas em

gerenciamento de projetos elaborado pelo PMI em 2013 que possui um capítulo específico sobre gestão de riscos. Este capítulo, conceituado pelo guia como uma área de conhecimento, orienta os principais processos, ferramentas e técnicas utilizados para planejar, identificar, analisar e monitorar os riscos de um projeto (Project Management Institute, 2013).

Segundo Hillson (2013a), os riscos somente são gerenciáveis quando identificados e documentados de forma clara e precisa; entretanto, a identificação de riscos produz apenas uma grande lista de riscos que é difícil de entender ou gerenciar. A EAR (Estrutura Analítica de Riscos) é uma ferramenta que permite agrupar e organizar os riscos de um projeto facilitando sua gestão (Hillson, 2003).

Como podemos observar, a gestão de riscos é essencial para garantir a solidez de um banco; contudo, somente os riscos identificados podem ser analisados e monitorados adequadamente. Se uma operação bancária está sujeita a regulamentação de órgaos externos, tais como Bacen (Banco Central do Brasil) e Auditorias Externas, e estes órgãos devem, entre outras funções, monitorar como os bancos estão controlando seus riscos, é factível que os riscos de projetos de desenvolvimento de software que envolvem bilhões de reais também sejam monitorados.

A questão de pesquisa deste estudo é agrupar e identificar os principais riscos envolvidos em uma carteira de projetos de desenvolvimento de software de um grande banco de origem brasileira. Essa visão será gerada utilizando-se a Análise de Conteúdo como técnica de análise de dados a partir de uma amostra de 359 registros de riscos de dezesseis projetos iniciados entre Mai/12 e Jul/13.

Sendo assim, este estudo se propõe a: (1) entender as semelhanças entre alguns modelos de referência de riscos de projetos; (2) identificar um modelo apropriado para categorizar e agrupar os riscos de projetos de desenvolvimento de software e; (3) identificar e analisar os principais riscos de uma carteira de projetos de TI em um grande banco brasileiro. O documento está organizado da seguinte forma: introdução, referencial teórico, metodologia, apresentação e discussão dos resultados, conclusões e recomendações.

2 REFERENCIAL TEÓRICO

Para o desenvolvimento deste estudo foram utilizados os fundamentos conceituais de três modelos de referência para a gestão de riscos, bem como os processos de identificação e documentação de riscos encontrados na literatura.

2.1 Modelos de referência para a gestão de riscos

As empresas se utilizam de modelos de referência para organizar seus processos gerenciais organizando assim seus modelos de gestão (Cardoso, 2008). O principal objetivo da gestão de riscos é fornecer informações que permitam tomar decisões conscientes sobre os fatores que podem dar errado em um projeto. Estas informações devem conter previsões de probabilidade e impacto dos riscos, além da análise de custos e benefícios sobre os controles que podem mitigar, transferir ou até mesmo eliminar estes riscos (Higuera & Haimes, 1996).

Na sequência apresenta-se: as dimensões da gestão de riscos e três modelos de referência de gestão de riscos onde o processo de identificação de riscos é comum a todos os modelos e destaca-se pela sua importância. Os modelos são apresentados do mais genérico para o mais específico: (1) o modelo da ISO é de utilização genérica e atende qualquer segmento de mercado; (2) o modelo do PMI é específico para gestão de projetos; e (3) o modelo do SEI é específico para o desenvolvimento de projetos de software.

2.1.1 Dimensões da gestão de riscos

Segundo Thamhain (2013) é possível destacar três grupos de variáveis interrelacionadas que devem ser consideradas na gestão de riscos e podem ser observadas na figura 1. Entender estas variáveis é importante para selecionar o modelo de referência para a gestão de riscos mais adequada, além das pessoas e organizações necessárias para lidar eficientemente com a situação de risco específica.

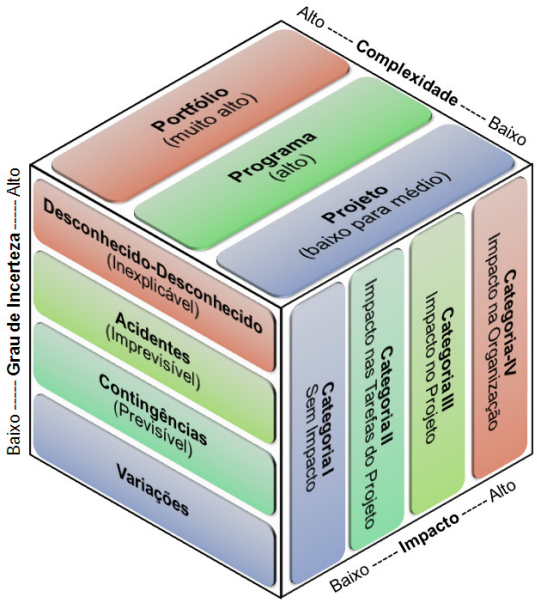

Figura 1: Dimensões da gestão de riscos.
Fonte: Adaptado de (Thamhain, 2013).

Grau de incerteza pode ser dividido em quatro categorias: (1) Variações das variáveis conhecidas do projeto, tais como custo, prazo ou requisitos. Podem ser controladas de forma eficiente pelas ferramentas convencionais de planejamento, execução e monitoramento do projeto; (2) Contingências são os eventos conhecidos que podem ocorrer e afetar negativamente o desempenho do projeto. Alguns métodos analíticos tais como PERT (*Project Evaluation and Review Technique*) e simulações ajudam a antecipar a materialização estes eventos; (3) Acidentes são eventos possíveis de serem identificados, mas a probabilidade e impacto são muito difíceis de serem previstos; e (4) Desconhecido-desconhecido são eventos vistos como impossíveis de acontecer dentro do contexto do projeto e passam a ser conhecidos pela equipe do projeto somente quando ocorrem.

Complexidade do projeto: existem diversos estudos que ajudam a classificar a complexidade de um projeto, sendo que o foco principal está baseado em dois aspectos: a "complexidade no projeto" que foca o ambiente organizacional, social e político e a "complexidade do projeto" que foca a dimensão do porte (tamanho) do projeto sendo este mais comumente utilizado e referenciado neste modelo como Projeto, Programa e Portfólio.

Impacto do risco no projeto e organização: apesar de projetos complexos serem susceptíveis a apresentar um impacto maior na organização, projetos

pequenos podem também impactar grandes segmentos do negócio. Sugere-se quatro categorias de riscos baseadas no impacto que estes podem gerar: (1) categoria I são os riscos que podem ser identificados e tratados antes mesmo de afetar o desempenho do projeto; (2) categoria II são os riscos que podem ser tratados e impactam um grupo de tarefas específico dentro do projeto; (3) categoria III são os riscos que impactam o desempenho do projeto, tal como atraso no prazo final e estouro do orçamento; e (4) categoria IV são os riscos cujo impacto extrapola o impacto no projeto e impacta a operação da organização, por exemplo, conforme reportado no Jornal Folha de São Paulo (2013) uma falha na implantação de um aplicativo simples do Banco do Brasil para Iphone e Android em 09/12/2013 permitiu que usuários tivessem acesso a extratos e a dados de outros clientes que também estivessem usando o aplicativo no mesmo momento.

2.1.2 ISO 31000 – Gestão de riscos

A ISO é a maior desenvolvedora de normas internacionais voluntárias do mundo. Foi fundada em 1947 e já desenvolveu mais de 19.500 normas abrangendo diversos aspectos de tecnologia e negócios. Tais normas são desenvolvidas por meio de um consenso entre especialistas de todo o mundo e oferecem o estado da arte em especificações de produtos, serviços e boas práticas (ISO, 2014).

Para as empresas, as normas internacionais facilitam o comércio mundial e a penetração em novos mercados, pois garantem que os produtos e serviços são seguros, confiáveis e de boa qualidade. Além disso, são ferramentas estratégicas que ajudam a tornar a indústria mais eficiente e eficaz, porque reduzem os custos, minimizam os erros e aumentam a produtividade (ISO, 2014).

Segundo a ISO (2009) todas as atividades de uma organização envolvem risco e este modelo apresenta os princípios e diretrizes genéricos sobre sua gestão. Conforme demonstrado na figura 2, as organizações gerenciam o risco, identificando-o, analisando-o e, em seguida, considerando seu apetite ao risco, avaliam se o risco deve ser modificado pelo tratamento do risco. Durante este processo, as organizações comunicam e consultam os envolvidos, além de monitorar e analisar o risco e os controles que o modificam, dessa forma procura-se assegurar que nenhum tratamento adicional seja necessário.

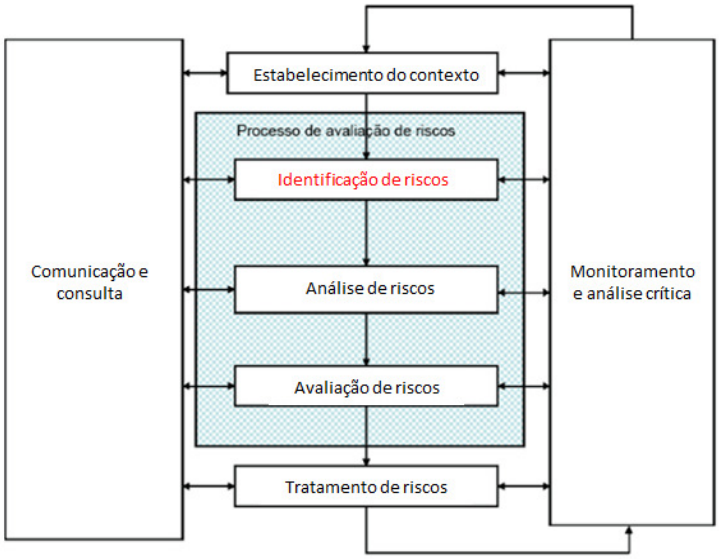

Figura 2: Modelo de referência para a gestão de riscos da ISO (ISO 31000).
Fonte: Adaptado de (ISO/ABNT, 2009).

A finalidade da identificação de riscos é gerar uma lista abrangente de riscos baseada nas incertezas que possam criar, aumentar, evitar, reduzir, acelerar ou atrasar a realização dos objetivos. Trata-se de um processo extremamente crítico, pois um risco que não é identificado nesta fase não será incluído em análises posteriores. Além de identificar o que pode acontecer, é importante considerar possíveis causas e cenários que mostrem quais consequências podem ocorrer. Convém que a organização aplique ferramentas e técnicas de identificação de riscos que sejam adequadas aos seus objetivos e capacidades e aos riscos enfrentados, além de envolver pessoas com conhecimento adequado sobre os riscos (ISO/ABNT, 2009).

2.1.3 PMI – Gestão de riscos de projetos

O PMI é a maior associação sem fins lucrativos no mundo de profissionais envolvidos com gestão de projetos, programas e portfólio. Fundado em 1969, o PMI contribui com mais de 2,9 milhões de profissionais que trabalham em quase todos os países do mundo por meio da educação e pesquisa. O PMI colabora com a melhoria do sucesso organizacional e amadurecimento da profissão de gestão de projetos por meio de seus padrões mundialmente reconhecidos, certificações, recursos,

ferramentas, pesquisas acadêmicas, publicações, cursos de desenvolvimento profissional e oportunidades de relacionamento entre os seus associados (Project Management Institute, 2014).

De acordo com o PMI (2013), os objetivos da gestão dos riscos do projeto são aumentar a probabilidade e o impacto dos eventos positivos e reduzir a probabilidade e o impacto dos eventos negativos no projeto. Conforme pode ser observado na figura 3, o modelo de referência para a gestão dos riscos é composto pelos processos de planejamento, identificação, análise qualitativa, análise quantitativa, planejamento de respostas e controle de riscos de um projeto.

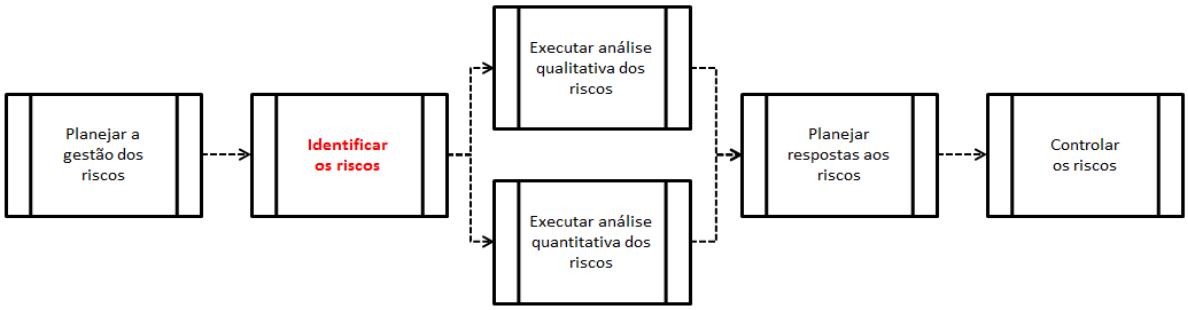

Figura 3: Modelo de referência para a gestão de riscos de projetos do PMI.
Fonte: Adaptado de (Project Management Institute, 2013).

Identificar riscos é o processo de determinação dos riscos que podem afetar o projeto e de documentação de suas características. O principal benefício desse processo é a documentação dos riscos existentes e o conhecimento e a capacidade que ele fornece à equipe do projeto de antecipar os eventos. Trata-se de um processo iterativo porque novos riscos podem surgir ou se tornar evidentes durante o ciclo de vida do projeto. Os riscos devem ser especificados de forma consistente para garantir que cada risco seja compreendido claramente e sem equívocos para permitir a análise e o desenvolvimento de respostas eficazes, além de permitir a comparação entre o efeito relativo dos riscos (Project Management Institute, 2013).

2.1.4 SEI – Gestão de riscos de projetos de desenvolvimento de software

O SEI é um centro de pesquisa e desenvolvimento financiado pelo governo federal dos Estados Unidos por meio de seu Departamento de Defesa e operado

pela Universidade Carnegie Mellon em Pittsburgh. O SEI trabalha em estreita colaboração com as organizações de defesa, governo, indústria e academia para melhorar continuamente os processos relacionados a engenharia de software e segurança de dados. Seu principal objetivo é ajudar as organizações a melhorar as suas capacidades de engenharia de software e desenvolver ou adquirir o software correto, livre de defeitos, dentro do orçamento e no tempo necessário. O SEI divulga suas tecnologias para a comunidade global de engenharia de software por meio de seus cursos públicos, conferências, relatórios técnicos e parceiros (Software Engineering Institute, 2014).

A metodologia de gestão de riscos em software foi proposta pelo SEI em 1996 e está aderente tanto ao *Acquisition-Capability Maturity Model (SA-CMM^{SM})* quanto ao *Software Capability Maturity Model (SW-CMMSM^{SM})*. Trata-se de uma metodologia que aborda todo o ciclo de vida de aquisição, desenvolvimento e manutenção do software, pode ser considerada uma metodologia madura, pois já foi implantada e testada em diversas organizações parceiras do SEI (Higuera & Haimes, 1996).

A figura 4 apresenta os processos deste modelo que são organizados de forma cíclica, apresentando a ideia de que tais atividades devem ser realizadas e revistas continuamente durante todo o projeto: identificar, analisar, planejar, monitorar, solucionar e comunicar os riscos. O processo de comunicação está no centro do modelo justamente para garantir a fluidez das informações entre os processos, pois é geralmente o maior obstáculo da gestão de riscos (Higuera & Haimes, 1996).

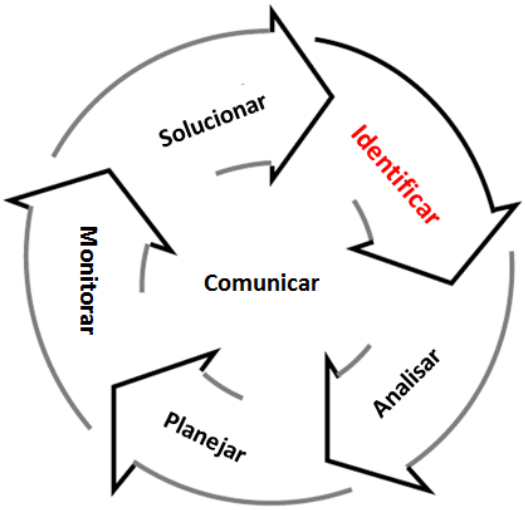

Figura 4: Modelo de referência para a gestão de riscos de projetos de tecnologia do SEI.

Fonte: (Higuera & Haimes, 1996).

O processo de identificação de riscos destaca-se dos demais, pois um risco somente pode ser analisado, planejado, monitorado e solucionado quando devidamente identificado. O SEI desenvolveu algumas técnicas para identificar as origens dos riscos em projetos de desenvolvimento de software, entre elas a Taxonomia de Riscos que será abordada em detalhes mais adiante (Higuera & Haimes, 1996).

2.2 Identificação de riscos

A total desinformação só existe até que as coisas aconteçam pela primeira vez. A partir daí, deixa de ser desconhecida, porque passa a existir informação histórica. A identificação de riscos é o início do processo de gestão de riscos e pode ser desenvolvido em três etapas: 1) analogia com projetos anteriores; 2) categorização de riscos – EAR; e 3) identificação de novos riscos (Salles Jr. et al., 2010).

A analogia com projetos anteriores significa buscar informações históricas sobre projetos de natureza semelhante que já foram realizados externamente ou internamente à organização; entretanto, observa-se que não existem bancos de dados históricos que permitam a analogia externa. Dessa forma, a correta identificação e documentação dos riscos é importante não apenas para o projeto, mas também para criar uma base histórica interna que servirá como fonte de consulta para novos projetos e gerará padrões para a organização (Salles Jr. et al., 2010).

A categorização de riscos consiste em agrupar os riscos por afinidade ou tipo e pode ser representada por meio de uma EAR. Por fim, depois de organizadas as informações sobre o projeto, a identificação de novos riscos é realizada utilizando-se ferramentas e técnicas de dinâmica de grupo (Salles Jr. et al., 2010), entre elas, podemos destacar o método de identificação de riscos baseado em uma taxonomia

(*TBRI – Taxonomy-Based Risk Identification*) elaborado pelo SEI para projetos de desenvolvimento de software (Carr, Konda, Monarch, Walker, & Ulrich, 1993).

2.2.1 Registro de riscos

Um projeto está sujeito a dois tipos de riscos: (1) riscos no projeto; e (2) riscos do projeto. Geralmente os gestores de projetos consideram somente os riscos no projeto que são os riscos individuais identificados e registrados no Registro de Riscos. Raramente são considerados os riscos do projeto que são os riscos associados com o escopo e benefícios do projeto onde se procura avaliar qual o impacto do projeto para a organização (Hillson, 2013b).

Um registro de riscos é uma ferramenta valiosa para compreender e gerenciar os riscos da organização, pois como não é possível gerenciar o que não se pode medir, o registro de riscos fornece um quadro com métricas que auxiliam a tomada de decisões com base em informações. Os principais benefícios de um registro de riscos são: a discussão em torno dos riscos relevantes que abrangem toda a organização; o registo é escrito usando linguagem interna para garantir que ele se relaciona com a organização em questão; e a conseqüência e probabilidade são mensuradas projeto a projeto (Mutton, 2012).

Geralmente os softwares de gestão de projetos possuem funcionalidades específicas para registro e monitoramento de riscos, mas também é possível organizar um documento de registros de riscos contendo as seguintes informações: número do risco, descrição do risco, categoria, causa, consequência, probabilidade, impacto, ação (evitar, mitigar, transferir ou aceitar), descrição do plano de ação, custo do plano de ação, evento que aciona o plano de ação e responsável (Mutton, 2012).

Por mais útil que seja, o registro de riscos não garante o sucesso do projeto se a ferramenta não for utilizada de forma adequada, e pode até mesmo prejudicar o desempenho do projeto. Três boas práticas que devem ser consideradas: (1) começar cedo: a capacidade de gerenciar e mitigar o risco do projeto é mais fácil no início de um projeto, pois uma vez que o projeto já tenha se iniciado e decisões tomadas, fica mais difícl e mais caro fazer mudanças; (2) durante a identificação dos riscos a contribuição de pessoas de diversas áreas (jurídico, vendas, tecnologia, recursos humanos, finanças, etc.) é muito valiosa, pois agrega diferentes

perspectivas na avaliação dos riscos; e (3) visitar e ravaliar os riscos regularmente, pois os riscos não são estáticos do início ao fim do projeto, os riscos são dinâmicos e podem mudar de um dia para outro (Guyer, 2012).

2.2.2 Estrutura analítica de riscos (EAR)

É uma técnica que permite agrupar possíveis causas de riscos. Podem ser usadas várias abordagens como, por exemplo, uma estrutura baseada nos objetivos do projeto por categoria. A estrutura analítica dos riscos ajuda a equipe do projeto a considerar muitas fontes a partir dos quais os riscos podem surgir em um exercício de identificação de riscos. Diferentes estruturas analíticas de riscos serão apropriadas para diferentes tipos de projetos. Uma organização pode usar uma estrutura de categorização previamente preparada, que pode ter a forma de uma simples lista de categorias ou ser estruturada em uma EAR. A EAR é uma representação hierárquica dos riscos, de acordo com suas categorias de riscos (Project Management Institute, 2013).

Uma lista de riscos identificados pode ser priorizada para determinar quais riscos devem ser endereçados primeiro, mas isso não permite compreender a estrutura de riscos do projeto. Uma EAR permite identificar temas recorrentes e áreas de concentração de riscos, além de servir como um guia para o processo de gestão de riscos. A melhor maneira de lidar com uma grande quantidade de dados é estruturar a informação para facilitar a compreensão. A EAR facilita a comunicação, a comparação com outros projetos e também serve como um documento de lições apreendidas para futuros projetos (Hillson, 2003). A figura 5 apresenta um exemplo de uma EAR.

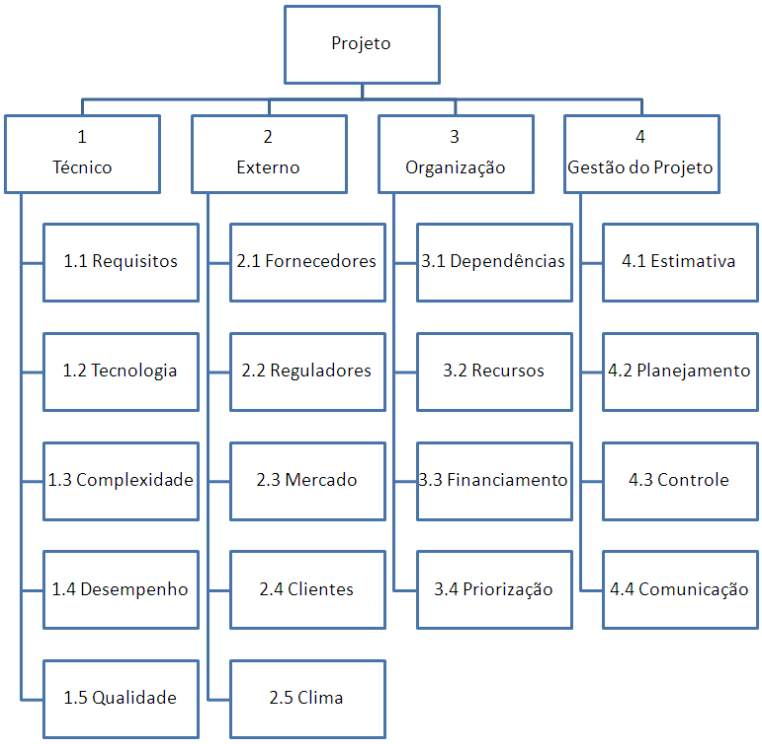

Figura 5: Exemplo de uma estrutura analítica de riscos.

Fonte: (Project Management Institute, 2013).

Cada organização pode criar a sua hierarquia de riscos. De uma forma bastante ampla e genérica, segundo Marshall (2002), uma possível hieraquia de riscos a ser adotada em uma instituição financeira pode ser a seguinte:

Risco de Crédito: risco de perdas associadas ao não cumprimento pelo tomador ou contraparte de suas respectivas obrigações financeiras nos termos pactuados, à desvalorização de contrato de crédito decorrente da deterioração na classificação de risco do tomador, à redução de ganhos ou remunerações, às vantagens concedidas na renegociação e aos custos de recuperação;

Risco de Imagem: risco de danos à reputação da instituição junto a clientes, concorrentes, órgãos reguladores, parceiros comerciais, entre outros, acarretando impactos no valor da marca;

Risco de Liquidez: risco de ocorrência de desequilíbrios entre ativos negociáveis e passivos exigíveis – "descasamentos" entre pagamentos e recebimentos – que possam afetar a capacidade de pagamento da instituição, levando-se em consideração as diferentes moedas e prazos de liquidação de seus direitos e obrigações;

Risco de Subscrição: risco oriundo de uma situação econômica adversa que contraria tanto as expectativas da sociedade seguradora no momento da elaboração de sua política de subscrição quanto as incertezas existentes na estimação das provisões;

Risco Estratégico: risco de implementar uma estratégia malsucedida ou ineficaz que fracasse em alcançar os retornos pretendidos;

Risco Operacional: risco de perdas resultantes de falha, deficiência ou inadequação de processos internos, pessoas e sistemas, ou de eventos externos. Inclui o risco legal, associado à inadequação ou deficiência em contratos firmados pela instituição, bem como a sanções em razão de descumprimento de dispositivos legais e a indenizações por danos a terceiros decorrentes das atividades desenvolvidas pela instituição;

Risco Socioambiental: risco de perdas em consequência de efeitos negativos no meio-ambiente e na sociedade decorrentes de impacto ambiental, impactos em povos e comunidades nativas e proteção da saúde humana, de propriedades culturais e da biodiversidade, quer sejam consequência das operações da própria instituição, quer sejam da concessão de financiamentos a projetos que não sejam desenvolvidos de forma socialmente responsável ou não reflitam boas práticas de gestão ambiental;

Risco de Projeto: é um evento ou uma condição incerta que, se ocorrer, provocará um efeito positivo ou negativo nos objetivos do projeto tais como custo, escopo, prazo ou qualidade (Project Management Institute, 2013).

2.2.3 *Taxonomy-based risk identification* (TBRI)

Os riscos em um projeto de desenvolvimento de software podem ser conhecidos, desconhecidos ou irreconhecíveis. Conhecidos são aqueles em que o pessoal do projeto está ciente, podem não estar explicitamente documentados, mas são acompanhados de alguma forma. Desconhecidos são aqueles que podem ser identificados utilizando-se técnicas que estimulem o mapeamento e discussão dos riscos. Irreconhecíveis são aqueles que ninguém poderia prever e estão fora do âmbito de qualquer método de identificação de riscos (Carr et al., 1993).

O TBRI é um método que auxilia na identificação dos riscos conhecidos e desconhecidos e é baseado nas seguintes premissas: os riscos de desenvolvimento de software são geralmente conhecidos pela equipe técnica, mas são mal comunicados; um método estruturado e repetitivo de identificação de riscos é necessário para garantir a gestão de riscos eficiente; e uma identificação de riscos eficaz deve cobrir todo o ciclo de vida do projeto (Carr et al., 1993).

A aplicação de um questionário semiestruturado (*TBQ - Taxonomy-Based Questionnaire*) orienta o gestor na coleta sistemática dos riscos junto à equipe do projeto. Os dados coletados são organizados e formam uma estrutura analítica de riscos padronizada e organizada em três classes principais: 1) *engenharia de produto* - são os aspectos técnicos do projeto (hardware, software e documentação); 2) *ambiente de desenvolvimento* - são os métodos, procedimentos e ferramentas utilizados para desenvolver o software; e 3) *restrições do programa* - são os fatores contratuais, organizacionais e operacionais externos ao projeto que estão fora da alçada do gestor, mas podem gerar impacto no sucesso do projeto (Carr et al., 1993). Na tabela 1 tem-se uma visão geral da estrutura.

Tabela 1

Visão geral da TBRI (Taxonomy-Based Risk Identification).

EAR – PROJETO DE DESENVOLVIMENTO DE SOFTWARE		
	A-Engenharia	
		1-Requisito: definição das funcionalidades, necessidades, comportamento e forma de utilização. Justificativa da viabilidade e estimativa de esforço. • Estabilidade – Os requisitos são estáveis? • Completude – Existem requisitos que deveriam estar nas especificações e não estão? • Clareza – É possível entender os requisitos da maneira como foram escritos? • Validade – O desenvolvedor e o cliente entendem a mesma coisa a partir dos requisitos? • Viabilidade – Existem requisitos tecnicamente difíceis de serem implementados? • Precedente – Existe algum requisito complexo? • Escala – O tamanho e complexidade do sistema são uma preocupação?
		2-Desenho: tradução dos requisitos em um projeto eficaz respeitando as restrições. • Funcionalidade – Existe algum algoritmo especificado que pode não satisfazer os requisitos? • Dificuldade – Alguma parte do modelo depende de premissas irreais ou otimistas? • Interfaces – As interfaces Software-Software e Software-Hardware estão bem definidas? • Desempenho – Existe alguma preocupação com o desempenho? • Testabilidade – Será fácil testar o software? • Restrições do hardware – O hardware limita sua habilidade para atender algum requisito?

EAR – PROJETO DE DESENVOLVIMENTO DE SOFTWARE
3-Código e Teste Unitário: tradução do desenho em código respeitando os requisitos em unidades individuais. • Viabilidade – Os algoritmos e desenhos especificados são fáceis de implantar? • Teste – Os testes unitários especificados e o tempo disponível para sua realização são suficientes? • Codificação/Implantação – As especificações dos desenhos estão suficientemente detalhadas para a codificação?
4-Integração: integração das unidades em um sistema e garantia de que o software atende os requisitos. • Ambiente – O ambiente de teste integrado/homologação permite simular cenários realistas para demonstrar os requisitos? • Produto – Os critérios de aceitação e formalização foram acordados para todos os requisitos? • Sistema – O software será integrado a outros sistemas existentes?
5-Especialidade: requisitos do produto ou desenvolvimento que exigem conhecimentos especializados, tais como segurança e confiabilidade. • Manutenção – A arquitetura, desenho ou código geram alguma dificuldade para a manutenção? • Confiabilidade – Foram especificados requisitos de disponibilidade? • Segurança – Será difícil verificar a qualidade dos requisitos de segurança? • Usabilidade – Existe alguma dificuldade no cumprimento dos requisitos de usabilidade?
B-Desenvolvimento
1-Processo: definição, planejamento, documentação, adequação, aplicação e comunicação dos procedimentos utilizados para desenvolvimento do produto. • Formalidade – Existe mais de uma metodologia de desenvolvimento de software (MDS) sendo usada? • Adequação – Foi necessário adaptar a MDS para este projeto/programa? • Controle do processo – É possível mensurar se a MDS está cumprindo suas metas de produtividade e qualidade? • Familiaridade – As pessoas estão familiarizados com a MDS? • Controle do Software – Há um mecanismo para rastreabilidade dos requisitos, desde a especificação até a implantação?
2-Método: ferramentas e equipamentos de apoio usados no desenvolvimento, tais como simuladores, ferramentas, compiladores e plataformas. • Capacidade – Há recursos suficientes para as fases de pico de demanda, tais como construção e testes? • Usabilidade – As pessoas entendem que as ferramentas de desenvolvimento são fáceis de usar? • Familiaridade – As pessoas já conhecem as ferramentas de desenvolvimento? • Confiança – As ferramentas de desenvolvimento são consideradas seguras? • Suporte – Existe suporte às ferramentas de desenvolvimento?
3-Gestor: experiência do gestor em planejamento e controle da comunicação, custo, escopo, prazo e qualidade de um projeto de desenvolvimento de software. • Planejamento – O projeto/programa está sendo gerenciado de acordo com o planejado? • Organização do projeto/programa – As pessoas entendem seus papéis e dos outros envolvidos no projeto/programa? • Experiência em gerenciamento – O projeto/programa possui gestores experientes? • Interfaces do projeto/programa – A gestão comunica os problemas nas alçadas competentes?
4-Gestão: métodos e ferramentas de apoio para gerenciar o projeto, tais como gestão de projetos, gestão de configuração, garantia de qualidade e gestão de pessoas. • Monitoramento – Há boletins de status periodicamente estruturados? • Gestão de pessoas – O pessoal está treinado de acordo com as competências requeridas para o projeto/programa? • Garantia de Qualidade – Existem mecanismos definidos para assegurar a qualidade? • Gestão da configuração – Existe um adequado sistema de gestão das configurações?

EAR – PROJETO DE DESENVOLVIMENTO DE SOFTWARE
5-Cultura: cultura organizacional onde o trabalho será realizado, incluindo as atitudes das pessoas e os níveis de cooperação, comunicação e moral. • Atitude de qualidade – O cronograma é suficiente para atender a qualidade esperada pelo cliente? • Cooperação – As pessoas trabalham cooperativamente através das fronteiras funcionais? • Comunicação – Há boa comunicação entre os membros do projeto/programa? • Moral – Há algum problema em reter as pessoas que você precisa?
C-Restrição
1-Recursos: restrições externas impostas com relação ao prazo, orçamento ou pessoal. Cronograma – Há dependências externas que podem vir a impactar o cronograma? • Equipe – Há alguma área em que as habilidades técnicas estão em falta (engenharia de software, análise de requisitos, arquitetura, desenho físico, desenho lógico, linguagens de programação, testes, gestão de configurações, garantia de qualidade, bases de dados, domínio da aplicação ou análise de desempenho)? • Orçamento – Há recursos ou funções sendo excluídos para reduzir o custo? • Instalações – As instalações de desenvolvimento são adequadas?
2-Contrato: termos e condições do contrato do projeto. • Tipos de contrato – Quais os tipos de contrato existentes no projeto/programa (preço fixo, custo + remuneração, etc.)? • Dependências – Há dependências de produtos externos ou serviços que podem afetar a qualidade, orçamento ou cronograma?
3-Interface: relacionamento com os clientes, áreas corporativas e fornecedores. • Cliente – O tempo de aprovação do cliente é adequado? O mecanismo para chegar a acordos com o cliente é efetivo? • Gestão executiva – A gestão do projeto/programa comunica os problemas para as alçadas competentes? • Fornecedores – Existe confiança nos fornecedores para entrega de componentes críticos? • Política – As políticas da organização estão afetando o projeto/programa?

Nota. Fonte: Adaptado de (Carr et al., 1993).

3 METODOLOGIA

Este estudo é uma pesquisa de abordagem exploratória de natureza qualitativa que utilizou a pesquisa bibliográfica e documental como estratégias de pesquisa. A unidade de análise é uma organização do setor bancário e as técnicas de coleta de dados utizadas foram a pesquisa documental e a análise de conteúdo.

A pesquisa exploratória tem como objetivo aprofundar o conhecimento sobre o problema a fim de torná-lo evidente (Gil, 2010). A questão de pesquisa deste estudo é agrupar e identificar os principais riscos envolvidos em uma carteira de projetos de desenvolvimento de software de um grande banco de origem brasileira. Trata-se de uma pesquisa que utiliza técnicas de avaliação qualitativas porque, segundo Martins & Theóphilo (2009), os dados coletados são predominantes descritivos (descrição dos riscos e plano de ação).

A unidade de análise é um dos maiores bancos brasileiros, permitindo assim, um entendimento razoável sobre o segmento de mercado. A organização não

autorizou a divulgação de seu nome, sendo assim, será referenciada neste estudo como Banco Beta.

A pesquisa bibliográfica utiliza fontes secundárias de dados e é fundamental para realizar pesquisas científicas de qualquer natureza, pois busca conhecer, analisar e discutir um assunto ou problema a partir de um referencial teórico. A pesquisa documental utiliza fontes primárias de dados, tais como documentos e bases de dados de entidades privadas, com o objetivo de contribuir para a análise dos problemas (Martins & Theóphilo, 2009). Por um lado, para entender teoricamente os principais modelos de referência para a gestão e categorização de riscos em projetos de software foram utilizadas fontes secundárias de dados como livros e artigos de renomados autores e instituições, por outro lado, para avaliar na prática como o Banco Beta trata essa questão, foi extraída uma base eletrônica de dados a partir da ferramenta corporativa de gestão de projetos.

Martins e Theóphilo (2009) assim explicam a análise de conteúdo: *"a Análise de Conteúdo adquire força e valor mediante o apoio de um referencial teórico, particularmente para a construção das categorias de análises. A categorização é um processo de tipo estruturalista e envolve duas etapas: o inventário (isolamento das unidades de análise: palavras, temas, frases etc.) e a classificação das unidades comuns, revelando as categorias"*. A coleta de dados foi realizada a partir de documentos internos e extração eletrônica de uma base de dados contendo o registro de riscos de alguns projetos de desenvolvimento de software iniciados a partir de Abril de 2012. Após a extração, os dados foram reduzidos e classificados conforme a taxonomia proposta pela literatura, utilizando os softwares Excel da Microsoft e NVivo da QSR.

A construção deste trabalho seguiu o seguinte roteiro:

Definição do tema, justificativa e objetivos;

Análise dos modelos de referência para a gestão de riscos;

Identificação e análise de uma Estrutura Analítica de Riscos específica para projetos de desenvolvimento de software;

Coleta de documentos e extração eletrônica de bases de dados;

Análise e interpretação dos resultados obtidos; e

Conclusão do trabalho, composto ainda por recomendações e limitações.

4 APRESENTAÇÃO E DISCUSSÃO DOS RESULTADOS

4.1 Contexto organizacional

O estudo foi realizado no Banco Beta, uma empresa privada, multinacional de capital nacional presente em 19 países além do Brasil, atuante no setor bancário de varejo e atacado desde 1943, possui atualmente 95.000 colaboradores, valor de mercado estimado em US$ 65 bilhões e conta com 5.000 agências e PABs no Brasil e exterior.

A área de tecnologia do Banco Beta possui investimentos previstos no valor de R$ 10,4 bilhões entre 2012 e 2015, conta com aproximadamente 6.000 colaboradores, um Escritório de Projetos de Tecnologia implantado e uma Área de Metodologia e Qualidade de Software que determina os padrões de processo a serem seguidos pelas equipes de desenvolvimento de software.

4.2 Resultados obtidos

Os dados para análise foram extraídos em Agosto de 2013 a partir do relatório de riscos gerado pela ferramenta de gestão de projetos utilizada pelo Banco Beta (Changepoint da Compuware Corporation). Após extração foram selecionados dezesseis projetos de desenvolvimento de software iniciados entre Maio de 2012 e Julho de 2013, cada projeto tinha mais de quinze riscos cadastrados gerando uma base de dados com 359 registros de riscos.

A classificação dos riscos foi realizada individualmente, ou seja, cada um dos riscos foi lido, interpretado e categorizado conforme a taxonomia proposta pelo SEI: (1) **Engenharia**: Requisito, Desenho, Código, Integração ou Especialidade; (2) **Desenvolvimento**: Processo, Método, Gestor, Gestão ou Cultura; e (3) **Restrição**: Recursos, Contrato ou Interface.

É importante destacar que a metodologia de gestão de projetos do Banco Beta foi elaborada utilizando como referência o guia PMBOK (*Project Management Body of Knowledge*) de boas práticas em gestão de projetos do PMI. Segundo o PMBOK (2013), os riscos identificados devem ser descritos com o maior número de detalhes possível e sugere-se utilizar a seguinte estrutura de descrição dos riscos: "*Se UMA CAUSA existe, o EVENTO pode ocorrer, levando ao EFEITO*".

Mesmo com as recomendações propostas pela metodologia de gestão de projetos da organização, durante a interpretação e classificação dos riscos observou-se falta de clareza na descrição dos riscos. Utilizando-se o software NVivo da QSR foi gerada a tabela 2 com a frequência das palavras mais utilizadas na descrição dos riscos. Pode-se observar que a descrição de 73 riscos (20%) mencionava algum tipo de atraso no prazo do projeto; entretanto, atraso não é um evento, mas sim o efeito negativo gerado por um risco. Dessa forma, foi necessária análise adicional dos planos de ação propostos para cada um dos riscos para permitir sua adequada categorização.

Nota-se também a falta de padronização, pois são utilizadas diferentes palavras para expressar o mesmo significado, por exemplo, para mencionar o prazo utiliza-se “prazo”, “prazos” e “cronograma”, ou seja, a falta de padronização além de gerar uma base histórica de lições aprendidas de baixa qualidade que dificulta pesquisas futuras, também indica a ausência de um modelo de referência maduro de gestão de riscos.

Tabela 2

Tabela da frequência de palavras.

Palavra	Qtd.	Palavras similares
atraso	73	atraso, atrasos
escopo	70	escopo
prazo	69	prazo, prazos
risco	64	risco, riscos
entrega	49	entrega, entregas
custos	45	custo, custos
sistema	45	sistema, sistemas
gerenciamento	42	gerenciamento
impactar	38	impactar
problemas	37	problema, problemas
falta	34	falta
mudanças	33	mudança, mudanças

Palavra	Qtd.	Palavras similares
plano	33	plano
qualidade	28	qualidade
atividades	25	atividade, atividades
durante	25	durante
processo	25	processo, processos
requisitos	25	requisito, requisitos
cronograma	24	cronograma
homologação	24	homologação
vulnerável	24	vulnerável
gestor	23	gestor, gestores
envolvidos	22	envolvidos
retrabalho	20	retrabalho

Nota. Fonte: Autor.

A figura 6 apresenta um gráfico de nuvem que destaca as palavras utilizadas com maior frequência na descrição dos riscos.

Figura 6: Gráfico de nuvem da frequência de palavras.

Fonte: Elaborado pelos autores.

Após categorizar todos os riscos foi possível agrupá-los utilizando o software MS-Excel. A tabela 3 apresenta a distribuição dos riscos conforme a taxonomia do SEI e a figura 7 o histograma da distribuição com a indicação do valor acumulado, permitindo assim, uma análise gráfica dos resultados do agrupamento.

Tabela 3

Tabela de distribuição dos riscos seguindo a taxonomia do SEI.

Categoria	Qtd.	%
A1 (Engenharia > Requisito)	81	23%
A2 (Engenharia > Desenho)	8	2%
A3 (Engenharia > Código)	0	0%
A4 (Engenharia > Integração)	31	9%
A5 (Engenharia > Especialidade)	9	3%
B1 (Desenvolvimento > Processo)	9	3%
B2 (Desenvolvimento > Método)	42	12%
B3 (Desenvolvimento > Gestor)	72	20%
B4 (Desenvolvimento > Gestão)	31	9%
B5 (Desenvolvimento > Cultura)	12	3%
C1 (Restrição > Recurso)	53	15%
C2 (Restrição > Contrato)	5	1%
C3 (Restrição > Interface)	6	2%
Total Geral	359	100%

Nota. Fonte: Elaborado pelos autores.

A figura 7 apresenta graficamente os resultados.

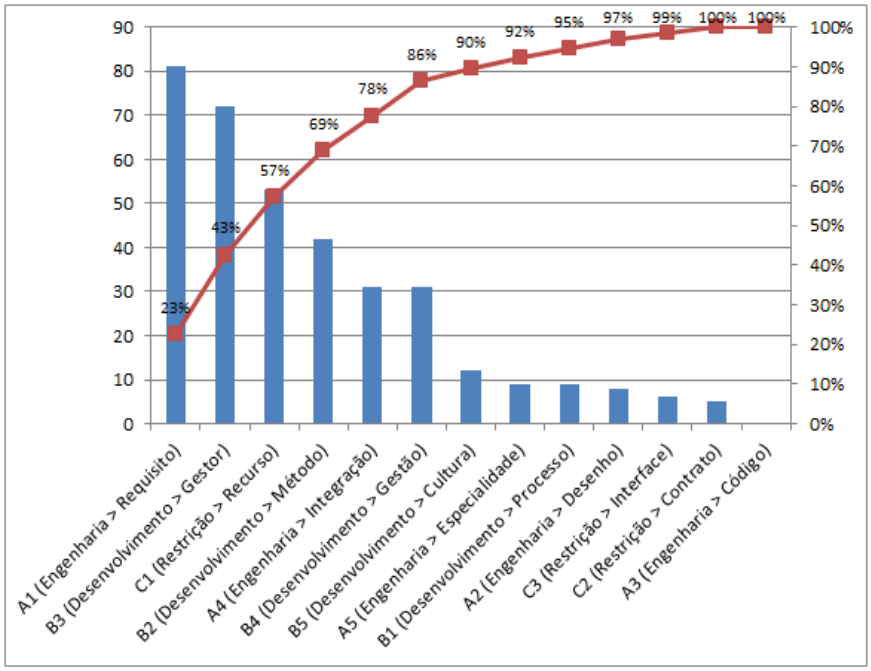

Figura 7: Gráfico de distribuição dos riscos seguindo a taxonomia do SEI.

Fonte: Elaborado pelos autores.

A partir da categorização dos riscos observa-se uma grande preocupação (69% dos riscos) dos gestores de projetos com relação à Definição de Requisitos, Experiência do Gestor, Restrição de Recursos e Métodos de Desenvolvimento. Por outro lado, os gestores de projeto não expressaram nenhuma preocupação relacionada à Codificação e Teste Unitário dos requisitos de software.

Analisando-se em detalhes os registros de riscos contidos nas categorias em destaque observa-se o seguinte:

(1) Definição de Requisitos: a codificação do software inicia-se mesmo com a falta de clareza dos requisitos, premissas e restrições. Como consequência destes riscos as estimativas de custo e prazo do projeto podem ser irreais e o software entregue pode não atender as expectativas do cliente. É fundamental para o sucesso de um projeto de desenvolvimento de software que os requisitos sejam estáveis, descritos de forma clara e completa, validados pelos desenvolvedores e tecnicamente viáveis.

(2) Experiência do Gestor: o principal risco identificado está relacionado com a dificuldade de planejamento do cronograma junto aos demais gestores funcionais. Gestores inexperientes podem ter deficiências em planejamento e comunicação e não devem ser líderes de projetos complexos que possuam diversas interfaces com sistemas legados, pois neste tipo de projeto é necessário negociar com os gerentes funcionais um cronograma adequado para todos os envolvidos e que atenda a necessidade do projeto. Além disso, é nessário garantir que esse cronograma se realize conforme planejado durante a execução do projeto.

(3) Restrição de Recursos: é recorrente o risco dos recursos humanos não estarem disponíveis para o projeto no momento adequado. Quando este tipo de risco se materializa, o atingimento do custo e cronograma planejado fica comprometido, principalmente quando o recurso humano está alocado em uma tarefa que pertence ao caminho crítico do projeto. Por isso é fundamental que nesta situação o plano de ação seja imediatamente acionado e a liberação ou substituição do recurso imediamente realizada.

(4) Métodos de Desenvolvimento: alto risco de instabilidade nos ambientes de teste integrado e homologação, tanto com relação às versões dos programas quanto com relação a baixa qualidade e baixo volume de dados para testes. As duas principais consequências deste risco são: (a) atraso no cronograma e/ou aumento dos custos durante a fase de testes, pois comos os testes não podem ser realizados na velocidade necessária, uma das possíveis soluções é aumentar o período de testes e/ou alocar mais recursos para realizar as tarefas desta fase; (b) baixa qualidade ao implantar o software em produção com alto volume de erros e possíveis prejuízos à organização.

Conforme pode ser observado na figura 8, a partir do agrupamento dos riscos, também é possível construir graficamente a EAR do portfólio de projetos selecionado para o estudo. Utilizando-se como referência a cor vermelho para os riscos elevados, amarelo para os riscos moderados e verde para os riscos baixos, obtêm-se uma EAR que apresenta graficamente as principais preocupações do portfólio de projetos, ou seja, os principais riscos recorrentes que devem ser monitorados frequentemente.

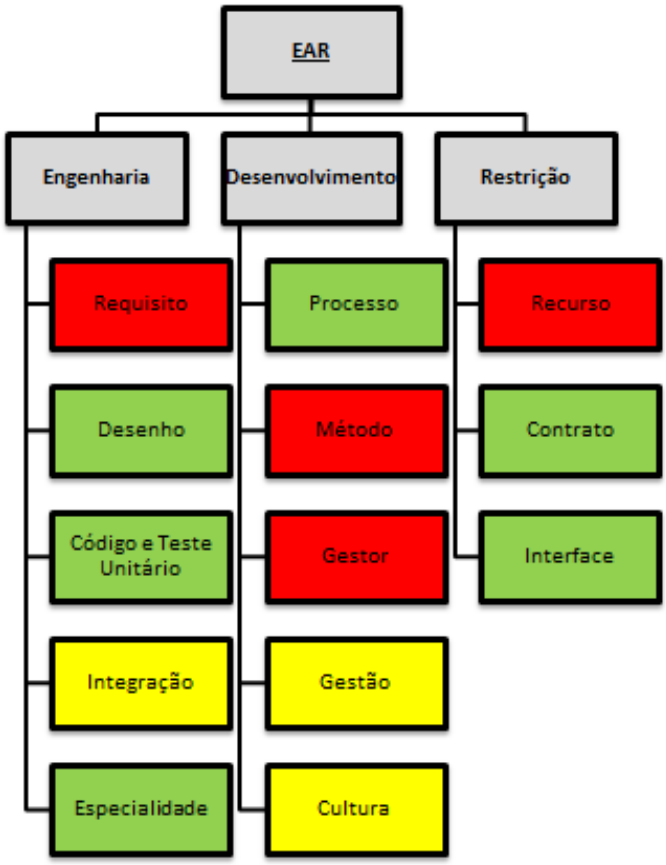

Figura 8: EAR do portfólio de projetos selecionados na amostra.

Fonte: Elaborado pelos autores.

5 CONCLUSÕES E RECOMENDAÇÕES

Com base no referencial teórico estudado podemos concluir que a fase de identificação de riscos é fundamental para a gestão de riscos, pois se o risco não for documentado, não será analisado, monitorado ou controlado, ou seja, riscos não identificados são riscos existentes, mas desconhecidos por toda a equipe do projeto.

Ficou evidente que os riscos são recorrentes em projetos de desenvolvimento de software. Uma metodologia para gestão de riscos e uma estrutura analítica de riscos padronizada facilitam a identificação e organização de riscos, além de permitir o agrupamento de dados para a geração de visões consolidadas da situação da organização que auxiliem a tomada estratégica de decisões. A taxonomia para categorização de riscos de projetos de desenvolvimento de software do SEI apresentou-se viável e flexível, portanto, poderia ser utilizada tanto na área de

tecnologia do Banco Beta quanto em qualquer outro Banco, garantindo a padronização da descrição dos riscos e eficiência na gestão dos riscos.

A categorização de riscos permite identificar e explorar problemas crônicos na organização. O estudo mostrou que o Banco Beta apresenta problemas com a gestão de requisitos, gestão de recursos e instabilidade nos ambientes de teste integrado e homologação. Um projeto pode iniciar a construção com uma parte do escopo ainda indefinido, desde que previamente acordado entre as partes; entretanto, este estudo demonstrou que tal comunicação e documentação não estão sendo eficientes. É muito importante que a metodologia de gestão de projetos proposta pela Área de Metodologia seja seguida de forma uniforme por toda a área de desenvolvimento de software, melhorando assim, a sinergia entre os projetos. Uma organização do tamanho do Banco Beta exige uma adequada gestão de recursos de modo que os gestores funcionais conheçam com precisão a alocação futura dos seus funcionários em outros projetos, evitando conflitos com os gestores de projeto. Também é fundamental que exista um ambiente de teste integrado e homologação íntegro que reflita com confiabilidade o ambiente produtivo e, dessa forma, garanta a qualidade esperada do software.

Respondendo a questão de pesquisa apresentada para este estudo, podemos concluir que é possível agrupar os riscos de uma carteira de projetos e identificar os principais riscos comuns aos projetos utilizando-se uma hierarquia de riscos padronizada.

Adicionalmente, foi possível verificar que atualmente os riscos não são agrupados ou categorizados nos projetos de desenvolvimento de software no Banco Beta, além disso, a descrição de riscos não é clara e precisa, dificultando a análise e controle do risco. Não existe documentação dos riscos organizada no formato de lições aprendidas, ou seja, não existe reaproveitamento dos riscos identificados em projetos anteriores. Podemos concluir que a gestão de riscos não é executada de forma padronizada no Banco Beta.

Fica a sugestão de que a taxonomia do SEI para categorização de riscos de projetos de desenvolvimento de software seja incorporada ao software de gestão de projetos da organização, além de um processo de capacitação e sensibilização dos gestores de projetos sobre a importância da adequada identificação, registro e classificação dos riscos. Este estudo pode ser expandido para outras empresas do

setor bancário, bem como para qualquer empresa que possua uma área interna de desenvolvimento de software.

O principal fator limitante para este estudo foi a utilização dos dados de apenas uma empresa do setor bancário.

REFERÊNCIAS

Realizado no formato APA 6ª edição utilizando o software Zotero (versão 4.0.12).

Cardoso, R. (2008). Construção de Modelos de Gestão Articulados por Modelos de Referência-Uma Investigação Sobre o Uso dos Modelos de Referência de Qualidade e Excelência. UFRJ.

Carr, M., Konda, S., Monarch, I., Walker, C. F., & Ulrich, F. C. (1993). Taxonomy-Based Risk Identification (No. CMU/SEI-93-TR-006) (p. 90). Software Engineering Institute. Retrieved from http://www.sei.cmu.edu/library/abstracts/reports/93tr006.cfm

Febraban. (2013). Relatório Anual Febraban 2012. Febraban. Retrieved from http://www.febraban.org.br/Relat%C3%B3rio_Anual_FBB_2012.pdf

Gil, A. C. G. (2010). Como elaborar projetos de pesquisa (5ª ed.). Atlas.

Gonzaga, Y. (2013, October 12). Falha em aplicativos do Banco do Brasil expõe contas de clientes. Folha online. São Paulo. Retrieved from http://www1.folha.uol.com.br/tec/2013/12/1383430-falha-em-aplicativos-do-banco-do-brasil-expoe-contas-de-clientes.shtml

Guyer, A. (2012). 3 Tips for Registering Risks. PM Network, 26(11), 61–61.

Higuera, R. P., & Haimes, Y. Y. (1996). Software Risk Management. Software Engineering Institute. Retrieved from http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=41707#

Hillson, D. (2003). Using a Risk Breakdown Structure in project management. Journal of Facilities Management, 2(1), 85–97. doi:10.1108/14725960410808131

Hillson, D. (2013a). [feedback]. PM Network, 27(1), 7–7.

Hillson, D. (2013b, October). Implicit and Explicit Risk Management. PM World Journal, p. 1.

ISO. (2014, March 6). Sobre a ISO. International Organization for Standardization. Retrieved from http://www.iso.org/iso/home/about.htm

ISO/ABNT. (2009). ISO 31000:2009 - Gestão de Riscos - Princípios e diretrizes. Multiple. Distributed through American National Standards Institute.

Marshall, C. (2002). Medindo e Gerenciando Riscos Operacionais em instituições Financeiras. Rio de Janeiro: Qualitymark.

Martins, G. de A., & Theóphilo, C. R. (2009). Metodologia da investigação científica para ciências sociais aplicadas (2ª ed.). Atlas.

Mutton, J. (2012). Do I really need a risk register? Keeping Good Companies (14447614), 64(8), 469–475.

Project Management Institute. (2013). A guide to the project management body of knowledge: (PMBOK® guide). Newtown Square: PMI.

Project Management Institute. (2014, March 6). Sobre o PMI. PMI. Retrieved from http://www.pmi.org/About-Us.aspx

Salles Jr., C. A. C., Soler, A. M., Valle, J. A. S., & Rabechini Jr., R. (2010). Gerenciamento de riscos em projetos (2ª ed.).

Software Engineering Institute. (2014, March 6). Sobre o SEI. Carnegie Mellon University. Retrieved from http://www.sei.cmu.edu/

Thamhain, H. (2013). Managing Risks in Complex Projects. Project Management Journal, 44(2), 20–35. doi:10.1002/pmj.21325