GESTÃO DE RISCOS: COMPREENSÃO DOS RISCOS E APLICAÇÃO DA GESTÃO[1]

Vitor Marciano

Resumo: Este artigo apresenta um estudo sobre a implementação de gestão de riscos empresariais e de projetos de TI, além das dependências entre eles. Em relação à teoria da gestão de riscos, foi explorada a necessidade de que o processo de gestão passe principalmente pelo fortalecimento da compreensão dos riscos e as ramificações que esta compreensão causa. Foi realizado um levantamento bibliográfico de implementações em empresas de grande e pequeno porte, sendo dois casos escolhidos para descrição neste artigo por representarem tanto o modelo desejado quanto a realidade da maioria das empresas. Foi dada ênfase para a gerência de riscos em instituições financeiras e as características peculiares a estes tipos de instituição, que fazem com que o tipo, a fonte e as características dos riscos sejam diferenciadas. As conclusões deste artigo encaminham à necessidade de compreender a gestão de risco no contexto empresarial como um todo.

Palavras-chave: Gestão, Risco, Tecnologia.

1 INTRODUÇÃO

Em um ambiente de desenvolvimento que se encontra em uma instituição financeira, existe uma gama enorme de fontes de risco que podem levar a situações que afetam a empresa negativamente tanto na sua imagem com seus clientes quanto em relação a prejuízos financeiros. Para mitigar estes riscos,é recomendável que sejam aplicadas técnicas e padrões de gestão de risco desde a definição das demandas de TI, passando pela implementação, e chegando até à execução dos serviços de TI.

---

1 Artigo apresentado como Trabalho de Conclusão do Curso de Especialização em 2017, da Universidade do Sul de Santa Catarina, como requisito parcial para a obtenção do título de Especialista em Gestão da Tecnologia da Informação.

Uma das principais dificuldades na implantação da gestão de riscos, é a conscientização da importância que todos os envolvidos nos processos de TI possuem na gestão de risco. Conforme:

> A crescente importância que a gestão dos riscos vem suscitando nas empresas reflete-se nas funções desempenhadas pela auditoria. As orientações de Turnbull, divulgadas pela Bolsa de Valores de Londres, estabelecem que todas as pessoas dentro de uma organização possuem, em graus diferentes, responsabilidades pela gestão do risco. Neste sentido, a auditoria, no papel de supervisão, contribui em garantir que o processo de gestão de risco esteja efetivamente funcionando. Para que o trabalho desenvolvido pela auditoria se revista de um caráter de agregação de valor, é adequado que ela emita parecer sobre a condução do processo de gestão de riscos pelos gestores. (POUCHAIN, 2007, p. 65).

Outro dificultador normalmente encontrado, é o fato de que copiar o que a literatura ou algum caso de estudo apresente como um caso de sucesso, não basta para atender às necessidades da organização, assim como explicitado em:

> Não existe uma definição de projeto que irá servir para qualquer situação. Todos os projetos são únicos em algum aspecto e diferenciam-se também das atividades relacionadas ao negócio normal da empresa. (SILVA, 2011, p. 16).

Atualmente, uma preocupação comum a quase todos os ramos de negócio é em relação à sua informatização, ou seja, seu investimento em TI. Isto se dá tanto pela necessidade de melhoria dos seus processos de produção e controle visando aumentar a competitividade da empresa, quanto para aumentar o seu alcance no mercado através da divulgação da sua marca, produtos, ou pela venda online. Silva (2011) trata do cenário em que o investimento em TI passa a ser quase tão importante quanto o investimento na atividade fim da empresa, e com isso a preocupação com os custos e retorno que estes investimentos terão no balanço da instituição.

Fernandes (2014) mostra a situação em que a governança e principalmente a gestão de riscos de TI passa a ser de extrema importância para que sejam definidos parâmetros confiáveis para a tomada de decisão sobre onde e quanto investir.

Em virtude do exposto, este estudo possui o objetivo de buscar o entendimento dos desafios encontrados na aplicação dos métodos de gestão de risco empresariais e de projetos de TI, assim como analisar as possíveis interdependências nestes processos. Para isso serão identificados os dificultadores para a implantação do modelo em uma instituição financeira, será verificada a existência de especificidades relativas à este tipo de instituição e por fim serão listadas as ações que devem ser tomadas para que os dificultadores sejam superados e a implementação seja bem sucedida.

Esta pesquisa possuirá o caráter de pesquisa aplicada pois propõe-se a realizar o levantamento baseado em tentativas concretas de implantação da gestão de risco empresarial e de TI. Por basear-se em ações concretas, esta pesquisa deverá ser empírica e com base em dados levantados diretamente ou registrados em documentação de implantações realizadas com caráter de pesquisa exploratória.

Conforme descrito, esta pesquisa partirá do pressuposto de que cada alvo da implementação da gestão de riscos possui características distintas, tanto no seu funcionamento interno quanto no tipo de problema a ser resolvido. Desta forma, o tipo de coleta de dados a ser utilizado será focado no tipo que considere cada situação como única, tornando esta uma pesquisa qualitativa.

Para o levantamento de dados, pretende-se realizar a análise de implantações dos processos de gestão de riscos empresariais e de TI com o intuito de analisar as características que levam ao sucesso ou fracasso das implementações e a relação entre elas.

O campo de pesquisa a ser adotado será primariamente a consulta bibliográfica da documentação relativa aos casos selecionados.

Finalmente, para a coleta de dados, será usada a consulta a documentos e bibliografias. Para o caso em que haja a pesquisa *in loco*, será aplicado um questionário ao profissional que tenha realizado a coordenação da implantação dos processos de gestão de riscos de TI na equipe estudada.

2 COMPREENSÃO E GESTÃO DE RISCOS

Antes de mais nada, torna-se importante que haja a definição do que constitui um risco para a empresa, após o que, pode-se levantar quais são os riscos de TI existentes para o contexto do(s) projeto(s).

> A definição utilizada pela ISO – International Organization for Standardization [38] trata o risco como "a combinação da probabilidade de um evento ocorrer e de suas consequências". Em suma, a combinação da probabilidade de ocorrência com o impacto causado. Particularmente, face às demais definições sobre gerenciamento de riscos que veremos no decorrer deste trabalho, entendo que a definição da ISO estaria mais apropriada para definir o grau de exposição a um risco. Para exemplificar, tomemos como exemplo a queda de um raio sobre um data center. O risco de queda de um raio sempre vai existir, é o que chamamos de ameaça natural. Entretanto, a combinação de algumas atitudes como a decisão sobre a localização do data center e a instalação de para-raios, que reduzem a probabilidade de queda de um raio sobre as instalações, bem como a instituição de backups e a existência de redundância de equipamentos, que reduzem o impacto

> (consequências), diminuem a exposição das instalações ao risco de queda de raio. (POUCHAIN, 2007, p. 31).

Conforme esta definição, vários fatores devem ser considerados para o levantamento dos riscos presentes em um determinado projeto de TI, estando estes fatores relacionados ao tipo de negócio, de infraestrutura e inclusive os fatores humanos.

Tem-se portanto que a combinação de eventos provenientes de incertezas e fatores humanos relacionados à execução das tarefas são variáveis que devem ser consideradas no levantamento dos riscos de um projeto.

Pouchain (2007) define que estas definições devem ser usadas para se chegar ao ponto onde haja a distinção de dois pontos na definição e tratamento dos riscos: a possibilidade de ocorrência de um evento e qual o impacto que esta ocorrência causará ao projeto.

Em relação às especificidades de um projeto quanto a definição de risco, deve-se levar em consideração quais as características da instituição onde a gestão de risco será colocada em prática, sendo necessário levar em consideração as necessidades do negócio bem como a sua relação com a área de TI. Estes fatores tornam-se importantes quando se analisa a maneira como o risco é percebido neste ambiente.

Silva (2011) relata a importância de que haja o entendimento de como os gestores percebem e compreendem os riscos dos projetos. Isto pois fatores emocionais, de habilidades individuais, crenças, experiências e diferenças de julgamento afetam a maneira como estes gestores são influenciados no momento das tomadas de decisão necessárias em situações onde a gestão de risco se dá necessária.

Eber (2006) descreve a diferença entre a percepção dos fatores de risco em projetos em um levantamento feito com a participação de diretores e gerentes de projeto. Neste levantamento houve uma enorme discrepância na percepção entre os dois grupos, sendo que os diretores identificaram como os cinco principais fatores de risco a falta de planejamento, plano de projeto não-realista, subestimar o escopo do projeto, alterações no cliente ou na gerência e por fim a falta de planejamento das contingências.

No mesmo estudo (Eber, 2006), os gerentes de projeto que foram ouvidos “elegeram” como os cinco principais fatores de risco as alterações no cliente ou na gerência, a complexidade técnica do projeto, plano de projeto não-realista, poucas pessoas na equipe e finalmente a inabilidade de detectar problemas antecipadamente.

Este levantamento mostra como os pontos de vista diferenciam-se de acordo com a área de atuação e demonstra como há a conscientização dos fatores que levam a falhas na implementação dos projetos.

É importante notar que a gestão de riscos não trata o risco apenas como algo ruim que deve ser identificado, tratado e evitado a qualquer custo, mas sim algo que possa alterar o andamento planejado e esperado de um projeto. Além de identificar o risco, deve-se analisar se deve ser tomada alguma ação caso o risco venha a se concretizar, conforme:

> Tendo como base o disposto anteriormente, prefiro chamar de "gestão do risco" a toda ação que vise minimizar ou mesmo conviver com o risco. Convém reforçar que conviver com riscos é também uma forma de gerir riscos. Um administrador, ciente dos riscos, do impacto e da probabilidade de ocorrência, pode decidir por não adotar nenhuma atitude e "correr o risco". A instituição de um determinado controle pode ser a resultante final do processo de análise de riscos. (POUCHAIN, 2007, p. 33).

Em instituições financeiras estas considerações devem ainda serem somadas às definições corriqueiras de riscos, outras definições que são especificas como por exemplo as regras que regem o acordo da Basiléia II, este estabelecido pelo *Bank for International Settlements* cuja sede situa-se na cidade suíça da Basileia.

Abreu (2014) cita que em virtude do Acordo da Basileia II, o Banco Central do Brasil passou a auditar as árias de TI dos bancos brasileiros de acordo com as regras definidas pelo CobiT – ISACA. Também é citada a importância do gerenciamento de risco em todas as facetas da atuação da TI visto que o Acordo da Basileia possui uma abrangência que cobre quase todos os elementos de TI em uma instituição financeira.

Estas definições específicas a instituições financeiras, culminaram com a emissão de resoluções por parte do Banco Central do Brasil que passaram a auxiliar na definição do conceito de risco em uma instituição financeira.

Em Abreu (2014) é reportado que a resolução 3380 do Banco Central do Brasil, publicada em junho de 2006, determina que as instituições financeiras do Brasil devem implementar suas próprias estruturas de gerenciamento de risco. Além disso, a resolução rege a definição do risco operacional para uma instituição financeira:

> Conforme definição na resolução, risco operacional é a possibilidade de ocorrência de perdas resultantes de falha, deficiência ou inadequação de processos internos, pessoas e sistemas, ou de eventos externos. No que tange à tecnologia da informação, a resolução refere-se a falhas em sistemas como risco operacional. Alguns riscos apontados, tais como interrupção de

> atividades da instituição e danos a ativos, também podem ser originados pela tecnologia da informação. (ABREU, 2014, p. 37).

Para que seja possível entender a existência dos riscos com uma maturidade que permita o seu tratamento de forma trivial, sem que ocorram situações que saiam do controle por fatores emocionais ou pessoais. Deve-se portanto, procurar entender por linhas gerais o processo de condução de um projeto de TI e seus riscos.

Em Silva (2011) é citado que apenas 25% dos projetos são considerados como casos de sucesso, onde houve a conclusão de todas as funcionalidades planejadas, houve a conclusão dentro dos prazos propostos e onde os gastos com o projeto não extrapolaram o previsto. Porém na prática este tipo de abordagem torna difícil a conclusão sobre o sucesso de um projeto, visto que a falha em um dos indicadores e dependendo do tamanho da extrapolação da falha não necessariamente torna o projeto em um projeto "fracassado" visto que as suas funcionalidades podem ter sido entregues de maneira satisfatória às necessidades de negócio da instituição.

Portanto para minimizar a possibilidade da ocorrência do fracasso no projeto, deve-se primeiramente realizar processos de controle e gerenciamento do ciclo de vida do risco.

Conforme Pouchain (2007) para cada ocorrência relacionada a um risco previamente identificado, deve-se decidir se haverá a "convivência" com o risco ou se um controle será implementado para mitigar o risco. No caso da implementação de um controle, estes podem estar enquadrados em três categorias: preventivos, detectivos e corretivos:

> Os preventivos são aqueles que agem anteriormente à consecução do risco. São exemplos deste tipo de controle: análise prévia dos antecedentes de um funcionário, quando de sua contratação; controle sobre o acesso físico de pessoas a ambientes; estabelecimento de segregação de funções em transações críticas etc. (POUCHAIN, 2007, p. 33).

> Os controles detectivos e corretivos entram em ação após a ocorrência de um evento e atuam em ambos os eixos da mesma figura. São exemplos desses controles: cálculos de hash, check points, planos de contingência, cópias de segurança de arquivos etc. O objetivo desses controles é detectar, o mais rápido possível, a ocorrência indesejada, procurando estancar o evento e ao mesmo tempo diminuir os impactos provocados. (POUCHAIN, 2007, p. 33).

Pouchain (2007) define o ciclo de vida do risco como um conjunto de fases compreendendo a identificação das situação de risco, análise da criticidade do risco, adoção de estratégias de controle e monitoramento da eficácia das medidas.

Os tipos de abordagem para gestão de riscos são tratados em Silva (2011) conforme três abordagens, avaliação, gestão e contingencial.

A avaliação se preocupa com a determinação dos fatores de risco, a gestão trata da coleta de informações para suporte à tomada de decisões e o contingencial trata das incertezas do ambiente

Junto aos tipos de abordagem citados, devem ser considerados também quais os modelos de mercado mais conhecidos na gestão de riscos, projetos e serviços de TI são usados pelas instituições tais como a Biblioteca de Infraestrutura de TI (ITIL), CobiT, o conjunto de normas ISO 10006, Rational Unified Process (RUP) e CMMI.

3 GESTÃO EM INSTITUIÇÃO FINANCEIRA DE GRANDE PORTE

O primeiro caso escolhido para embasar a argumentação deste trabalho, é relativo à aplicação da gestão de riscos em uma grande instituição financeira canadense, apresentado em Fraser (2015), implantação esta que apresentou características que representam as ideias e padrões encontrados durante o estudo realizado.

O *TD Bank Group* é uma instituição financeira canadense de grande porte, com atuação em várias partes do mundo. Esta instituição realiza suas operações com o suporte de mais de 85.000 funcionários espalhados em suas unidades.

Para o gerenciamento de risco na instituição, foi estabelecido um sistema de gerenciamento (ERF - *Enterprise Risk Framework,* Sistema de Riscos Empresariais) que trabalha a gerência de riscos através da identificação da natureza e do tipo de riscos que a empresa está exposta, além de prover as definições de como os riscos são gerenciados dentro da instituição.

O primeiro passo tomado é a definição e a geração da declaração de apetite de risco que contém a quantidade de riscos que a empresa está disposta a correr, sendo que esta quantidade é definida com base na missão da empresa, visão, princípios além da sua filosofia de gerenciamento de riscos definida pelo ERF.

Também durante a definição do apetite de risco, é definido que estes riscos devem estar de acordo com as estratégias de negócio, não podem ser riscos que possam gerar perdas significativas em um único evento e principalmente que eles não levem a prejuízos à imagem da empresa e com consequente perda de confiança do mercado e clientes, algo de extrema importância para instituições financeiras.

Outras características importantes que são levadas em consideração quanto ao apetite versus risco, se dá por causa de especificidades relativas à instituições financeiras e o que é considerada uma característica chave na classificação de um risco quanto a ele ser um risco de capital, risco de liquidez, risco de mercado e risco operacional.

Durante a gerência de riscos no TD BANK, boas práticas são aplicadas quando se trata da realização da identificação dos riscos nas atividades do dia a dia da organização, após o que são tomadas medidas para garantir que estas atividades estão gerando riscos que estão contidos nos limites aceitáveis de gerenciamento da instituição. Após estas ações, são disparadas atividades de criação de controle de risco e que visam a reportar as características do risco para que seja possível a sua classificação e posterior monitoramento do seu ciclo de vida.

A estrutura da gerência de riscos é definida de forma a balancear o controle centralizado com a responsabilização por parte das áreas da empresa. Neste cenário, existem os comitês executivos que são responsáveis por dar suporte aos tomadores de decisão, suporte este que visa facilitar para que os mesmos possam atender às necessidades da empresa, ao mesmo tempo em que tomam decisões cujos riscos estejam contidos dentro das características e criticidades esperados pelas estratégias de gerenciamento de risco definidas pelas definições do ERF e do apetite de risco.

Para atender este balanceamento, existe a definição de uma estrutura hierárquica na gerência de risco compreendendo um gerente de riscos (CRO - *Chief Risk Officer*), sendo que a este se reportam os executivos de risco de cada unidade de negócio. Estas funções são responsáveis pela definição da gerência de risco de uma forma proativa e que dissemine a cultura do gerenciamento de riscos por toda a organização.

Como suporte à esta hierarquia e ao CRO, existe o cargo de auditor, o qual se encarrega de assegurar que os processos de governança, controle e gerência de riscos mantêm a empresa dentro dos limites de risco planejados.

Esta hierarquia também é responsável por se assegurar alguns princípios tais como o gerenciamento de riscos possuir como escopo, toda a empresa, inclusive o relacionamento com os parceiros comerciais; a existência de um processo de comunicação transparente e efetivo, onde os assuntos relativos aos riscos identificados são comunicados de forma clara e são escalados de forma ágil às gerências; garantir que

os riscos identificados no processo, são devidamente entendidos quanto à sua classificação e características; fazer com que os empregados da organização estejam cientes dos riscos relacionados a suas atividades e se responsabilizam por eles tanto de forma individual como de forma coletiva; assegurar que a gestão de riscos esteja integrada ao cotidiano da empresa em todos os níveis, tanto na forma de conscientização e orientação quanto via o fornecimento de ferramental e treinamento.

Em relação à área de tecnologia do TD Bank, existe a definição de um programa de controle e gerenciamento de riscos tecnológicos e de segurança da informação, cujo intuito é principalmente a proteção dos funcionários e clientes do banco através do uso de controles empresariais que procuram disseminar a cultura da prevenção de riscos e troca de informações além de, no nível empresarial, fomentar as ações de gerenciamento de vulnerabilidades e incidentes de TI.

Dentro da estrutura de gerenciamento de riscos definida, existem processos regulares de monitoração e apresentação das estatísticas e níveis de risco através de painéis que provêm indicadores sobre a quantidade e "qualidade" dos riscos identificados. Junto a estes indicadores são apresentados alertas para situações onde ocorram alterações nos riscos monitorados assim como o surgimento de riscos não previstos.

Estes painéis possuem perfis de informação que estão alinhadas às definições do ERF quanto as capacidades e tolerância a riscos definidas, sendo também de extrema importância no apoio à tomada de decisão em todos os níveis gerenciais e para as redefinições anuais da declaração do apetite de risco pelos níveis mais altos da hierarquia da gestão de riscos.

Uma característica presente na atividade de instituições do ramo financeiro em relação ao gerenciamento de risco e suas definições definições, é a necessidade de que várias informações de risco gerenciadas pelo TD Bank devam ser informadas a órgãos reguladores visto que algumas das diretrizes a serem seguidas durante o processo são definidas externamente à organização.

Observa-se portanto uma empresa com alto nível de maturidade, em todos os seus níveis hierárquicos, no gerenciamento de riscos.

4 GESTÃO EM EMPRESA DE TI DE PORTE MÉDIO

O segundo caso, relatado em Silva (2011), se refere a uma empresa de porte médio sediada em Porto Alegre/RS pertencente a um grupo multinacional, cuja atuação se dá no fornecimento de soluções de TI a empresas no Brasil e exterior e onde é aplicada metodologia formal de desenvolvimento através de processo próprio baseado no PMI. O Processo de desenvolvimento possui certo grau de maturidade inclusive com certificação CMMI® nível 3.

O projeto de estudo foi a customização de um sistema de ERP de um cliente de grande porte com sede na Europa, cujo sistema necessitava de uma evolução em um dos módulos. O retorno previsto pelo cliente pelas melhorias solicitadas foi de aproximadamente 10 milhões de reais.

Foi definido que durante o projeto, a comunicação entre as duas empresas seria realizada entre os gerentes de projeto apontados por cada uma como responsável pela implantação das alterações, sendo importante notar que as duas empresas já possuíam relação anterior para alterações no mesmo sistema ERP, mas apesar disso, houveram dificuldades na obtenção de informações sobre o negócio na visão do gerente de projetos da empresa contratada.

O projeto teve a duração prevista para 12 meses (setembro de 2009 a novembro de 2009) porém teve conclusão após um período de 16 meses (março de 2010).

Durante a negociação do projeto, foi enviado um documento de proposta onde constam os riscos preliminares ao projeto, levantado pela empresa contratada sendo que mais riscos poderiam ser incluídos posteriormente.

Na fase de iniciação foram realizados levantamentos para a definição dos riscos ao projeto, porém não são definidas as metodologias para este levantamento, tampouco metodologias para a gerência dos mesmos.

Uma das principais dificuldades durante a execução do projeto, foi a ação de definição dos detalhes das regras a serem alteradas no sistema, sendo que esta responsabilidade foi repassada à equipe de desenvolvimento da empresa contratada.

Com o projeto contendo um atraso de 50% em relação ao prazo inicialmente estipulado, foi iniciada a homologação do mesmo, porém devido ao atraso não havia disponibilidade da equipe responsável pela homologação por parte da empresa contratante visto esta fase estar acontecendo em um momento posterior ao previsto.

Assim que houve disponibilização de pessoas por parte da equipe da empresa contratante, houve indisponibilidade de equipe por parte da empresa contratada para desenvolver o projeto pois a equipe de desenvolvimento original havia sido alocada em outro projeto, e após negociação entre as empresas, houve a realocação de membros da equipe original que estavam em outro projeto possibilitando assim que a homologação e entrega do projeto fosse realizada, porém causando impactos no outro projeto cujo atendimento a empresa contratada necessitou comprometer.

Em relação ao gerenciamento de riscos durante o projeto, foi verificado que não foram definidos métodos ou regras para a realização desta gerência. Apenas oi definido que deveria haver o gerenciamento dos riscos, porém sem qualquer ferramental ou metodologia adequada.

Durante o desenvolvimento o gestor de negócio da empresa contratante foi incumbido de reportar semanalmente os dados relativos aos riscos identificados durante o projeto, tais como a probabilidade de que um determinado risco previamente identificado ocorra, atribuindo uma porcentagem entre 0% e 100%, o status dos riscos identificados, o andamento da gestão dos riscos, isto é, que ações estão sendo tomadas para a realização da gestão dos riscos, as estratégias adotadas em relação a cada risco e quais ações o gestor prevê no caso de mitigação ou contingência.

Durante o projeto foi verificado com o gerente de projetos da empresa contratada, que havia pressão para que fosse feito o gerenciamento de riscos, porém a ele não foi informado quais as práticas deveriam ser adotadas. Soma-se a isto, o fato de que o levantamento de riscos foi realizado por cada integrante do projeto levando-se em consideração apenas a visão do próprio integrante em relação ao que deveria ser considerado um risco em uma atividade.

Sobre os riscos, foram inicialmente identificados três riscos, sendo eles o risco de atraso no inicio do desenvolvimento por falta de definição clara das regras de negócio, o atraso no inicio dos testes de homologação do sistema e o atraso na entrega.

Posteriormente foram identificados e inseridos mais dois riscos um deles sobre problemas de alocação de profissionais para a homologação do sistema e o outro relativo a indefinição do escopo do projeto devido a alterações nas regras de negócio.

Importante salientar que estes dois últimos riscos foram identificados apenas após a ocorrência dos mesmos, portanto não houve gerência ou tratamento dos mesmos.

Por fim, a gestão dos riscos foi realizada por parte do gerente de projetos da empresa contratada, sendo que esta gestão foi realizada de acordo com suas necessidades e preferências o que fez com que ações de gestão de risco tomadas, acabassem gerando novos riscos. Como exemplo, para mitigar o atraso no inicio do desenvolvimento por falta de definição de regras claras, foi tomada a decisão de dar início ao desenvolvimento e complementar as regras durante o projeto o que foi o catalisador para a ocorrência do risco de indefinição de escopo do projeto.

5 CONCLUSÕES

Após o estudo do primeiro caso TD BANK caso, conclui-se que a organização possui um nível alto de maturidade e comprometimento em relação ao gerenciamento de riscos não só por necessidade própria mas também por imposição mercadológica em função do tipo de negócio praticado e externa por parte de órgãos reguladores. Outro fator importante a ser notado é o comprometimento da empresa com o gerenciamento de risco em todos os níveis de atuação e a sua disseminação, o que vai de encontro às necessidades para implantação da gerência de riscos conforme:

> Alinhar a gestão de riscos de TI com o sistema de gestão de riscos da organização: significa que a gestão de riscos da TI deve ser integrada com a gestão de riscos da organização. Em organizações com governança corporativa madura, é estabelecido um sistema de gestão de riscos operacionais já com metodologias estabelecidas e com mapas de risco por processo de negócio ou por serviços (no caso de bancos, o sistema de gestão de riscos abrange riscos de crédito, riscos operacionais e de mercado). (FERNANDES, 2014, p. 185).

No segundo caso apresentado, vê-se o caso oposto ao apresentado na primeira pois além da organização não ter nenhuma definição de metodologia para o gerenciamento de risco, não há qualquer sinergia entre a gestão de riscos realizada no projeto com as necessidades tanto da empresa contratante, empresa detentora do negócio, como da empresa contratada para prestar os serviços de TI.

Isto ficou evidenciado na ocorrência de um atraso de 50% para um projeto cujo escopo envolvia alterações nos sistemas da empresa, em funcionalidades cuja melhoria levavam a projeção de um lucro da ordem de R$ 10.000.000,00 para a empresa, sem que o atraso nestas melhorias fosse mensurado em quaisquer indicativos de risco na empresa contratante.

Esta situação apresentada foi ponto comum em vários casos estudados durante os levantamentos para este artigo, principalmente quando existe a relação contratante e

contratado e também quando há alocação de equipes de tamanho reduzido para a condução de projetos.

Relacionando os casos foi concluído que a gestão de riscos de TI deve ser implementada de acordo com uma visão maior de riscos dentro de uma organização, independente de a equipe responsável pelos serviços de TI ser interna ou contratada externamente. Isto significa que processos e estruturas de gestão bem definidos devem ser apresentados como um plano que englobe toda a instituição, fazendo com que a gestão de riscos de TI seja apenas uma parte da gestão de riscos empresariais e não uma aplicação contida em si mesma.

Esta necessidade se apresenta ainda mais em empresas de grande porte visto as diversas fontes de risco apresentadas em seus diversos departamentos e/ou unidades. No caso de instituições financeiras estas necessidades se multiplicam, uma vez que além das várias normas de diversos órgãos regulamentadores, os fatores de risco podem implicar em consequências com impacto não somente localizado à instituição, dependendo do tipo de ocorrência como por exemplo um incidente resultante de um projeto de TI que cause a indisponibilidade de vários serviços de um banco para a seus clientes por um tempo que cause impactos econômicos que podem ir do local, passando pelo regional até impactos globais.

REFERÊNCIAS

FERNANDES, Aguinaldo A.; ABREU, Vladimir F. **Implantando a GOVERNANÇA de TI: da Estratégia à Gestão dos Processos e Serviços**. Rio de Janeiro: BRASPORT, 2014.

FRASER, John R.S.; SIMKINS, Betty J.; NARVAEZ, Kristina. **Implementing Enterprise Risk Management: Case Studies and Best Practices**. New Jersey: WILEY, 2015.

POUCHAIN, Adriano de Melo. **GESTÃO DE RISCOS APLICADA AO AMBIENTE INTERNET BANKING DAS INSTITUIÇÕES FINANCEIRAS DO BRASIL**. Brasilia, 2007. Disponível em http://www.dominiopublico.gov.br/pesquisa/DetalheObraForm.do?select_action=&co_obra=94990. Acesso em 31/03/16.

SCHMITZ, Eber A.; ALENCAR, Antonio J.; VILLAR, Carlos B. **Modelos Qualitativos de Análise de Risco para Projetos de Tecnologia da Informação**. Rio de Janeiro: BRASPORT, 2006.

SILVA, Priscila Coelho da. **Análise da gestão de riscos em projetos de sistemas de informação**. Porto Alegre, 2011. Disponível em http://www.lume.ufrgs.br/handle/10183/29982. Acesso em 31/03/16.