O uso de melhores práticas de gerenciamento de riscos em um projeto de implantação de sistema ERP em uma empresa de manufatura[1]

Wagner Pereira[2]

Resumo: No mundo dos negócios, as inúmeras e aceleradas transformações aumentam a disputa de espaços e de clientes. Fato é que o volume de informações é transmitido em grandes quantidades e velocidade, com o desenvolvimento das tecnologias em curto espaço de tempo. O estudo tem como objetivo apresentar ferramentas para minimização de falhas em ambientes de TI, utilizando como guia frameworks de gerenciamento de riscos. Aproveita-se como referência, artigos e autores que contribuíram para o tema, além de frameworks de governança como o COBIT® 5. No estudo também apresenta-se o caso em uma empresa do segmento de manufatura observado pelo autor. Por fim, a pesquisa mostrou o valor da gestão de riscos para as organizações, e também a relevância que o tema tem, fornecendo de forma satisfatória para empresas, organizações, líderes e gestores de TI, como um meio de conscientização ou um método para aplicação dessas práticas.

Palavras-chave: Frameworks, Governança de TI; COBIT, ERP, Riscos em TI.

1 INTRODUÇÃO

Gerenciar e manter um ambiente de Tecnologia da informação (TI) seguro tem sido um grande desafio para organizações de médio e grande porte atualmente. Mesmo com o avanço de ferramentas de gerência e novas tecnologias, as organizações estão expostas aos riscos. Vesely (1984, p.103) enfatiza que “o risco pode ser entendido como o perigo, probabilidade ou possibilidade de um infortúnio, insucesso ou resultado indesejado”. A necessidade das empresas em conhecer os riscos dos seus processos de negócio passou a constituir um fator estratégico para o sucesso dos seus negócios, as empresas bem-sucedidas entendem e gerenciam os riscos do seu negócio e as suas limitações da TI, de modo ao equilíbrio adequado entre as oportunidades de ganhos e a minimização de perdas em uma organização.

Uma boa governança corporativa permite que as organizações trabalhem com eficiência e de forma produtiva, garantindo a transparência da responsabilidade gerencial tanto em organizações privadas com no setor público (AKABANE, 2012).

A preservação da integridade, confidencialidade e disponibilidade dos dados é um fator primordial para a proteção dos ativos da organização, por isso o gerenciamento de riscos evita o impacto negativo de segurança como perda ou degradação de qualquer uma das propriedades de segurança (integridade e disponibilidade), ou, então, pela combinação delas. (LENTO, 2012)

Sendo assim, para minimizar os riscos em ambientes de TI, podemos empregar *frameworks* baseados em COBIT (*Control Objectives for Information and related Technology*) (MARK, 2013, p. 56).

> O COBIT *(Control Objectives For Information and Related Technology)*, é uma estrutura de governança de TI e um conjunto de frameworks *(ferramentas)* de suporte que permite aos gerentes preencher a lacuna entre requisitos de controle, problemas técnicos e riscos de negócios (MARK, 2013, p. 113)

Considerando esse contexto, apresenta-se neste trabalho um estudo de caso real na implementação do gerenciamento de riscos (GR) em uma organização no segmento de manufatura, que necessitou desenvolver um projeto complexo de implantação de um novo sistema de ERP (*Enterprise Resource Planning*). No caso apresentado o software legado em uso era insuficiente para atender as demandas existentes e a empresa enfrentava vários problemas relacionados a ele. No projeto desenvolvido utilizou-se as melhores práticas de gerenciamento de segurança para garantir sucesso na implementação. Assim sendo, o presente artigo tem por finalidade apresentar ferramentas e soluções capazes de minimizar os riscos de TI, utilizando frameworks baseados em COBIT, aplicadas a um estudo de caso real. O foco principal desse artigo, portanto, é descrever como os frameworks de governança foram utilizados no caso abordado, com menor ênfase na descrição dos riscos propriamente ditos. Dada essa delimitação, destaca-se que alguns riscos são descritos como uma forma de exemplificar a metodologia adotada, sem a pretensão de esgotar a descrição de todos os riscos envolvidos no projeto.

2 ASPECTOS METODOLÓGICOS

A parte inicial dessa pesquisa caracteriza-se como bibliográfica, uma vez que utiliza como fontes livros, artigos de internet, artigos de jornais e revistas sobre o tema.

“A pesquisa bibliográfica é o estudo sistematizado desenvolvido com base em material publicado em livros, revistas, jornais, redes eletrônicas, isto é, material acessível ao público em geral”. (VERGARA, 2005, p. 48).

Esta pesquisa também caracteriza-se como um estudo de caso, desenvolvido em uma organização de manufatura. A coleta de dados no campo de estudos baseou-se na observação de seu autor, pois este fez parte do quadro de colaboradores da organização, respondendo diretamente à diretoria estratégica da empresa. Segundo Bruney et al. (*apud* DUARTE e BARROS, 2006, p. 216) no estudo de caso faz-se uma “análise intensiva, empreendida numa única ou em algumas organizações reais.” No entendimento dos autores, o estudo de caso agrupa, tanto quanto possível, informações numerosas e detalhadas para atingir a totalidade de uma situação. Essa foi a abordagem adotada no presente estudo.

3 REFERENCIAL TEÓRICO

3.1 Gerenciamento de risco de TI (GRI)

No atual cenário os frequentes ataques que comprometem os processos do negócio de uma organização via o comprometimento de serviços ou indisponibilidade aos dados do sistema computacional são diversos e eficazes, quando não combatidos. Esses incidentes adversos são aqueles que proporcionam uma consequência negativa, como inviabilizar o uso de sistemas. (SCARFONE ET AL, 2008 *apud* BRITO, 2010). Sendo assim, o impacto negativo de um evento de segurança pode ser descrito em termos de perda ou degradação de qualquer uma das propriedades de segurança (integridade e disponibilidade), ou, então, pela combinação delas.

Desta forma, o gerenciamento de risco de segurança da informação possibilita que a organização mantenha a sua informação protegida e disponível em tempo hábil, de forma que os seus processos de negócio estejam ativos e a sua missão seja cumprida.

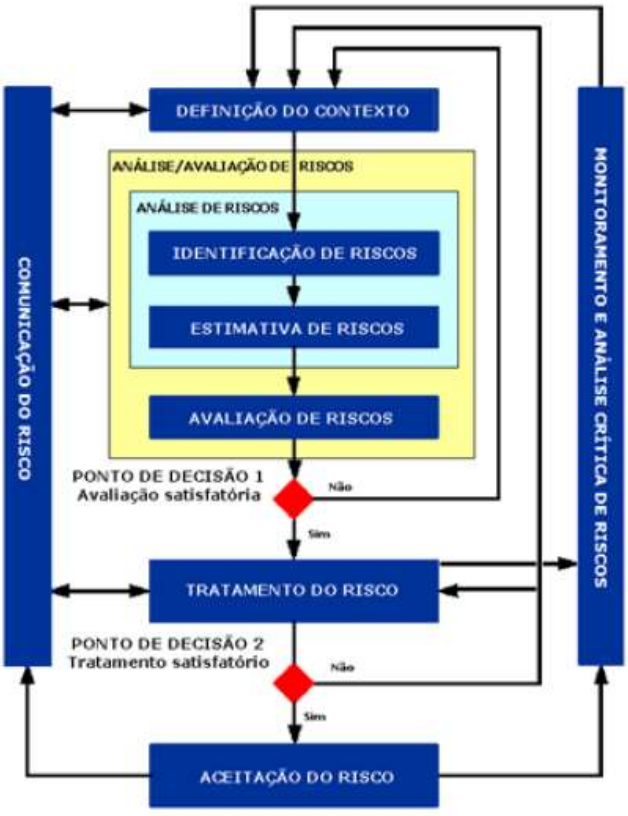
Para Stoneburner et al (2002, p. 146)

> A gestão de riscos é o processo de identificação dos riscos, avaliação de risco e tomada de medidas (tratamento do risco) para reduzir o risco a um nível aceitável. O objetivo da gestão de risco é permitir que a organização consiga realizar as suas tarefas, isto é, manter os seus

processos de negócio ativos através de uma melhor segurança para os sistemas de TI, responsáveis em armazenar, processar e transmitir as suas informações.

A norma ISO/IEC 27005 (ABNT, 2008) define risco como o potencial de uma determinada ameaça explorar vulnerabilidades, proporcionando perdas ou danos a um ativo ou grupo de ativos, de forma direta ou indireta, para a organização. A Figura 1 apresenta a relação entre as sete etapas do processo de gestão de risco e seu tratamento para determinar uma solução ou aceitação do risco.

Figura 1 – Processo de gestão de riscos segundo a norma ISO 27005



Fonte: ABNT (2008, p. 05)

Para auxiliar gestores na gestão de riscos existem diversos *frameworks* de Gestão de TI, direcionados especificamente para isso, como: O Guia *Project Management Body Of Knowledge* (PMBOK), Risk IT (information technology) e o Val IT. Há também os

códigos de boas práticas de segurança da informação da ABNT (Associação Brasileira de Normas Técnicas): ISO/IEC 27002, ISO/IEC 27005, e também o COBIT 5 (2012).

A Gestão de Riscos (GR) é definida pelo ISACA (2012),

> "um dos objetivos da governança. Implica o reconhecimento do risco; avaliação do impacto e da probabilidade daquele risco; e desenvolvimento de estratégias para evitar o risco, reduzir o efeito negativo do risco e/ou transferir o risco, para administrá-lo no contexto da organização de inclinação ao risco" (ISACA, 2012, p. 95).

Mark (2013) define GR como conceitos básicos, identificação e avaliação de ativos, definição de ameaças e análise de riscos, e processos e mecanismos para proteger os ativos. Em seu núcleo, a prática da segurança aborda a redução dos riscos para os ativos a níveis aceitáveis, usando um método abrangente e abordagem para que o risco ainda seja mitigado e controlado mesmo quando um controle falha. O Quadro 1 apresentar uma breve descrição de cada um dos *frameworks* citados neste trabalho.

Quadro 1 - *Frameworks* de Governança de TI e Gerenciamento de Riscos

COBIT 5	A última edição (2012) da biblioteca de governança de TI do ISACA (Information Systems Audit and Control Association), que ajuda gestores nas tomadas de decisões dos negócios de TI.
RISK IT	*Framework* fundamentado em COBIT 5, que tem como abrangência todos os fatores do gerenciamento de riscos, norteando gestores no tratamento e relatar os riscos de TI.
ISO/IEC 27002	Código de boas práticas para gerenciamento de segurança da informação que de acordo com a ABNT tem como principal objetivo: "estabelecer diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização (ABNT, 2005)."
ISO/IEC 27005	Norma técnica que abrange Gestão de Riscos de Sistemas de Informação. É um dos requisitos da norma ISO/IEC 27002, no qual surgiu complementando como um desdobramento.
VAL IT	Norma técnica que abrange Gestão de Riscos de Sistemas de Informação. É um dos requisitos da norma ISO/IEC 27002, no qual surgiu complementando como um desdobramento.
PMBOK	Norma técnica que abrange Gestão de Riscos de Sistemas de Informação. É um dos requisitos da norma ISO/IEC 27002, no qual surgiu complementando como um desdobramento.

Fonte: elaborado pelo Autor (2018)

3.1.1 Definições e benefícios dos frameworks de gestão de riscos

A mensuração da performance é essencial para a governança de TI, e identificar os processos e controles críticos relacionados à mesma são fundamentais para que os executivos possam eleva-los ao nível de capacidade desejado. Com isso emerge a preocupação com a integridade e segurança da informação. Para que haja a mitigação do impacto de vulnerabilidades, foram desenvolvidas boas práticas de gerenciamento de riscos. Os *frameworks* são conjuntos de práticas que visam padronizar os processos de TI dentro de uma organização, e representam grande subsídio para que os planos de gestão de riscos tenham sucesso.

Entre esses *frameworks* existem normas e metodologias que guiam o desenvolvimento de uma gestão de riscos, que fornecem um conjunto de diretrizes distintas para o gerenciamento dos riscos. Dentre os modelos de referência para gestão dos riscos que visam nortear as implementações necessárias estão a estrutura da série ISO 27000 que combina a avaliação inicial de risco com controles essenciais para a conformidade com as regulamentações típicas e controles considerados e melhores práticas comuns para segurança da informação. Os controles de melhores práticas incluem a criação de um documento de política de segurança da informação, desenvolvimento de um plano responsabilidades de segurança claramente definidas, educação e treinamento em segurança, relatórios e desenvolvimento de um plano de recuperação de desastres (BECKERS et al, 2011, p. 327)

A norma ISO 27002 (ABNT, 2005) é um conjunto detalhado de controles de segurança da informação que idealmente impulsionada pela saída da avaliação de risco realizada como parte da ISO 27001. Este padrão forma uma importante referência para as organizações sobre padronização e boas práticas de segurança. Enquanto a Norma ISO 27005:2008 trabalha em conjunto e define uma estrutura de gerenciamento de riscos para segurança da informação ser usado para informar as decisões dentro da ISO 27001 que levam à seleção de controles para a ISO 27002 (LENTO, 2012, p. 75). Ambas podem trabalhar ligadas e se tornam ferramentas extremamente eficazes se seguidas à risca.

Destaca-se também à ferramenta PMBOK© que é um guia de referência que descreve o conjunto de conhecimento dentro da área de Gestão de Projetos e gerenciamento de riscos, ou seja, ele descreve o conhecimento e as práticas que são

aplicáveis à maioria dos projetos e quanto ao gerenciamento de risco, sendo um amplo consenso a respeito de seu valor e utilidade (PMI, 2013).

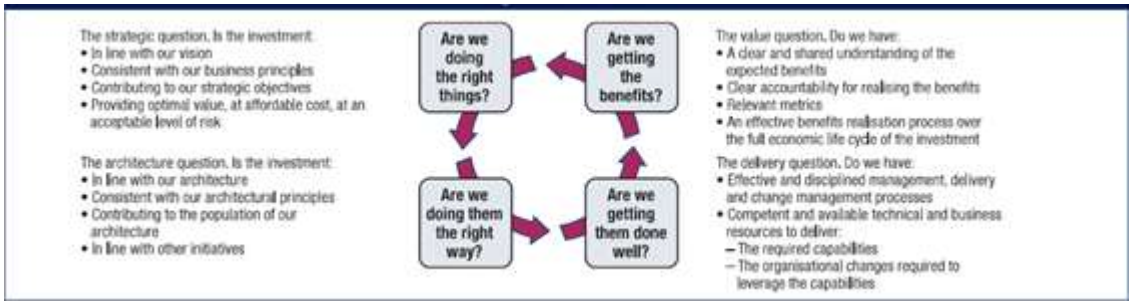
Este guia reúne também as práticas inovadoras e avançadas para todas as áreas de conhecimento que envolvem projetos: escopo, prazo, custo, recursos humanos, comunicação, qualidade, contratação, riscos e integração. Assim sendo, gerenciar riscos é fundamental para o sucesso de seu projeto, pois dessa maneira é permitido monitorar e controlar vários aspectos do projeto, procurando desvios e tendências para identificá-los precocemente. Outra vantagem de se fazer esse tipo de gerenciamento é manter as partes interessadas a par dos progressos e andamentos do projeto.

O framework *Risk IT* complementa o COBIT. Foi criado com o objetivo de ajudar os gerentes a relatar os riscos de TI, fornecendo uma estrutura abrangente para o controle e governança de soluções e serviços baseados em tecnologia de informação (TI). Embora o COBIT estabeleça boas práticas para os meios de gerenciamento de riscos, fornecendo um conjunto de controles para mitigar os riscos de TI, o *Risk IT* define boas práticas para os fins, fornecendo uma estrutura para empresas para identificar, administrar e gerenciar riscos de TI. A estrutura *Risk IT* deve ser usada para ajudar a implementar a governança de TI e as empresas que adotaram (ou estão planejando adotar) o COBIT como sua estrutura de governança de TI pode usar a TI de risco para aprimorar o gerenciamento de riscos (ISACA, 2011).

O *framework Val IT* fornece suporte direto para executivos em todos os níveis de gestão, em todos os negócios e organizações de TI, a partir do CEO e outros líderes até os gerentes e administradores, diretamente envolvidos nos processos de realização da seleção, aquisição, desenvolvimento e implantação dos benefícios. O *Val IT* tem um objetivo de criar valor ao negócio através dos investimentos nos habilitadores de TI, desenhado estreitamente e alinhado com o COBIT®, primeiramente fornece uma estrutura abrangente para a entrega de informações de alta qualidade serviços baseados em tecnologia (baseados em TI). Embora o COBIT estabeleça boas práticas para os meios de contribuindo para o processo de criação de valor, a Val IT estabelece boas práticas para os proporcionando às empresas a estrutura de que necessitam para medir, monitorar e otimizar realização de valor de negócio do investimento em TI (IT Governance Institute, 2008)

O *Val IT* ajuda os executivos a se concentrarem em duas das quatro questões fundamentais relacionadas à governança de TI (Figura 2): "Estamos fazendo as coisas certas?" (A questão estratégica) e "Estamos obtendo os benefícios? “Questão de valor), são perguntas que são realizadas para tomada decisão estratégica que o gestor tem que realizar comparando o negócio da empresa versus resultados esperados. O COBIT, por outro lado, assume a visão de TI, ajudando os executivos a se concentrarem em responder perguntas "Estamos fazendo caminho certo?" (A questão da arquitetura) e "Estamos fazendo isso bem? '(a questão da entrega).

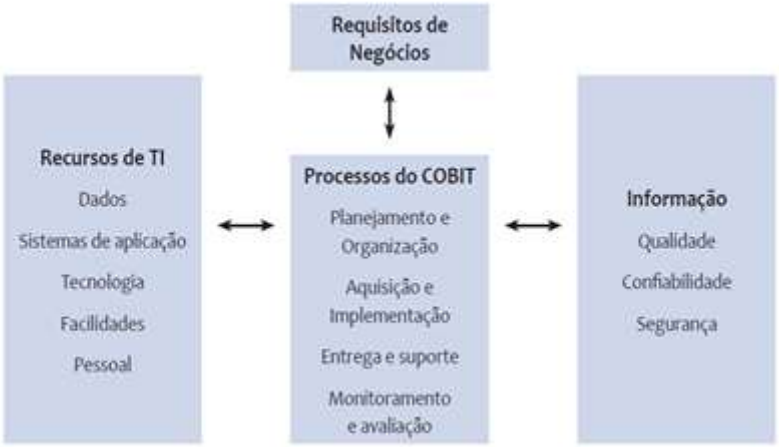
Figura 2 – Quatro perguntas na decisão de estratégica de TI



Fonte: IT Governance Institute (2008)

Sendo o COBIT integrador dos *frameworks* de governança e de gestão, ele auxilia as organizações a fim de obter as melhores práticas de Governança e Gestão de TI. Segundo (VIEIRA, 2007, p.22), “os objetivos de controle do COBIT procuram atestar como cada processo faz uso dos recursos de TI para atender de forma primária ou secundária a cada requerimento do negócio em termos de informação, cobrindo todos os seus aspectos. ” A Figura 3 apresenta uma visão geral do COBIT. Nela observa-se a ênfase com os requisitos de negócios e suas três principais dimensões.

Figura 3 – Visão geral do *framework* COBIT.



Fonte: BECKERS et al (2011, p. 95)

A execução das iniciativas relacionadas a negócios de entrega, integração e operação de mudança de negócios estão fora do escopo da TI governança (ou seja, COBIT), mas estão dentro do escopo de governança corporativa de TI (ou seja, Val IT) (VIEIRA, 2007, p.28).

Comparando como o COBIT e o Val IT se concentram em governança, processos e portfólios, pode-se perceber a relação entre esses dois referenciais O Quadro 2 apresenta essa comparação.

Quadro 2 - Comparação do Val IT com o COBIT

	Foco Governança	Foco de Processo	Foco de Portfolio
VAL IT	Governança corporativa de TI	➢ Projeto e iniciação de programas. ➢ Realização de benefícios ➢ Fornecer a visão geral do desempenho do portfólio. ➢ Aspectos de investimento e gerenciamento de valor contínuo de todos os processos.	➢ Gerenciar o portfólio de investimentos ➢ Fornecer a visão geral do desempenho do portfólio
COBIT	Governança de TI	➢ Entrega de soluções de TI ➢ Programas de investimento em implementação operacional de TI ➢ Entrega de serviços de TI	➢ Gerenciar o portfólio de projetos de TI em apoio a programas de investimento ➢ Gerenciar os portfólios de serviços, ativos e outros recursos de TI ➢ Fornecer informações sobre o desempenho dos portfólios de serviços, ativos e outros recursos de TI.

Fonte: IT Governance Institute (2008) – tradução do autor

COBIT 5 é uma estrutura única e integrada, porque integra todos os conhecimentos anteriormente dispersos em diferentes *frameworks* da ISACA, tais como o COBIT 4.1, Val IT (valor de TI para o negócio), Risk IT (risco relacionado ao uso de TI), BMIS (segurança). Está alinhado com os mais atuais e relevantes padrões e *frameworks* utilizados na governança corporativa e de TI.

Apresenta-se nos Quadros 3 e 4 os benefícios do COBIT para as organizações e seus princípios essenciais.

Quadro 3: Benefícios do COBIT

Manter	Informações de alta qualidade para suportar as decisões de negócios; Riscos com a TI em um nível aceitável; A conformidade com leis, regulamentos, acordos contratuais e políticas.
Gerar	"Valor" dos investimentos em TI, ou seja, atingir metas estratégicas e entregar benefícios de negócio por meio do efetivo uso da TI;
Atingir	A excelência operacional por meio da aplicação confiável e eficiente da tecnologia;
Otimizar	Otimizar o custo de serviços de TI;

Fonte: adaptado pelo autor (2018).

Quadro 4 Princípios do COBIT

1	**Atender as necessidades dos stakeholders**	Atingir o alinhamento estratégico entre TI e o resto da organização é um elemento crítico do COBIT, no qual constitui obter benefícios por meio da otimização do uso de recursos e dos riscos a um nível aceitável.
2	**Cobrir a organização de ponta a ponta**	Cobrir todas as funções e processos de uma organização não somente TI, mas trata a informação e tecnologias relacionadas como ativos que precisam ser tratados como qualquer outro ativo da organização
3	**Aplicar um *framework* único e integrado**	O COBIT® serve como um *framework* abrangente para a Governança Empresarial de TI
4	**Possibilitar uma abordagem holística**	Um sistema organizacional requer a definição e aplicação, de uma maneira holística, de estruturas e processos, assim como aos aspectos ambientais e culturais (pessoas, cultura, valores, etc.)
5	**Separar a governança de gestão**	No COBIT® declara-se pela primeira vez que os processos de governança de TI e de gerenciamento de TI referem-se a diferentes tipos de atividades

Fonte: adaptado pelo autor (2018).

Destaca-se que utilizar o COBIT associado com *VAL IT* e *RISK IT pode-se trazer* bons resultados para organização. E para obter melhores práticas na segurança da informação no geral pode-se utilizar-se da Norma ISO/IEC 27002 e ISO/IEC 27005. Quanto a gestão de risco e sucesso na implantação ou metodologias de projeto o PMBOK pode orientar na busca da melhor saída no quesito controle do projeto (PMI, 2013).

Assim, uma forma de estabelecer um padrão de governança que atenda e alinhe os objetivos de TI aos objetivos estratégicos das organizações e a introdução de melhores práticas em tecnologia da informação na forma de minimizar e elencar os riscos de TI, os conjuntos de *frameworks* conduzem esse caminho adequadamente.

3.1.2 A resistência às mudanças e barreiras culturais

A cultura da organização possui uma grande influência em todo o contexto da implantação de projetos tecnológicos. É preciso distinguir os aspectos culturais da organização, pois as decisões estratégicas adotadas são produtos dos padrões e valores da empresa, partes integrantes da sua cultura organizacional. Uma implantação de um sistema ERP, por exemplo, pode ser avaliada, em muitos casos, como uma mudança

perturbadora, pois altera os processos organizacionais, transformando a relação entre os colaboradores e até mesmo a maneira de se conduzir negócios (ESCRIVÃO et al, 2002).

O fator humano é principal propulsor nos aumentos dos custos, devido à tendência natural da maioria das pessoas em identificar após fechamento do escopo novos riscos no qual não foram relatados. Assim o uso do *Framework* PMBOK, pode ajudar construir um conjunto de etapas de mudança, que incluem a responsabilidade de fazer acontecer com sucesso, dentro dos prazos e orçamentos estabelecidos, respeitando os aspectos humanos envolvidos, deve ser associada a um método de que gera a eficácia e motivação satisfatória para anular a inércia e a resistência. Sugere-se uma equipe especialmente voltada para a realização das etapas e correção, auxiliar os desvios e resistência à mudança (PMI, 2013).

3.1.3 Etapas da implementação do gerenciamento de riscos

Devido a governança de TI englobar diferentes metodologias, frameworks, padrões do mercado e melhores práticas reconhecidas internacionalmente, para alcançar perfeita harmonia entre a TI e o negócio da organização, apresenta-se as etapas importantes para minimizar os riscos no ambiente corporativo.

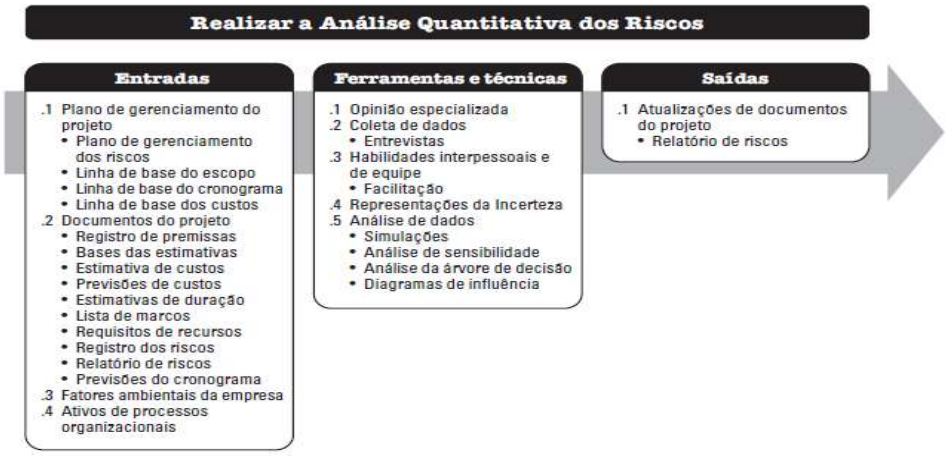
3.1.3.1 O Mapeamento de Riscos

Conforme metodologia do Framework do PMI (PMBOK, 2013) o mapeamento de riscos se divide em três etapas gerenciais e duas análises técnicas utilizadas para coleta de dados sendo:

- Monitoração dos riscos: é o processo que tem como objetivo identificar e assegurar o controle desses, monitorando os residuais e identificando novos que possam vir a surgir, assegurando a execução dos planos do risco e avaliando sua eficiência na redução desses.
- O gerenciamento de riscos: auditores de risco (responsáveis pelo risco) examinam e documentam a eficácia da resposta ao risco, concentrar os maiores esforços nas etapas de planejamento em relação às etapas de controle, pois a execução do projeto passa a ser prioritário, relatórios periódicos e boa comunicação

- Acompanhamento dos riscos: revisões periódicas dos riscos nas reuniões com a equipe do projeto, monitoramento os riscos residuais, identificação dos novos riscos, execução de planos de respostas a riscos e avaliação da sua eficácia durante todo o ciclo de vida do projeto.
- A Análise Quantitativa dos Riscos: tem como objetivo avaliar a exposição ao risco para priorizar os riscos que serão objeto de análise ou ação adicional, os riscos com maior probabilidade e impacto são priorizados para posterior criação de um plano de respostas, os riscos com menor probabilidade e impacto são mantidos nos registros dos riscos dentro de uma lista de observação para monitoramento futuro, avaliação de probabilidade e impacto de riscos; matriz de avaliação da urgência. As entradas e saídas deste processo estão ilustradas na Figura 4.

Figura 4 – Processos de análise quantitativa dos riscos.



Fonte: PMI (PMBOK, 2013, p. 276)

- Análise Qualitativa dos Riscos: é realizar a análise quantitativa dos riscos tem como objetivo efetuar a análise numérica do efeito dos riscos identificados nos objetivos gerais do projeto, por envolver alta complexidade, é realizada somente nos riscos priorizados pela análise qualitativa, técnicas de representação e coleta de dados: entrevistas; distribuições de probabilidades; opinião especializada; análise quantitativa de riscos e técnicas de modelagem. As entradas, ferramentas e técnicas e saídas desse processo estão ilustradas na Figura 5.

Figura 5 – Processos de análise qualitativa dos riscos

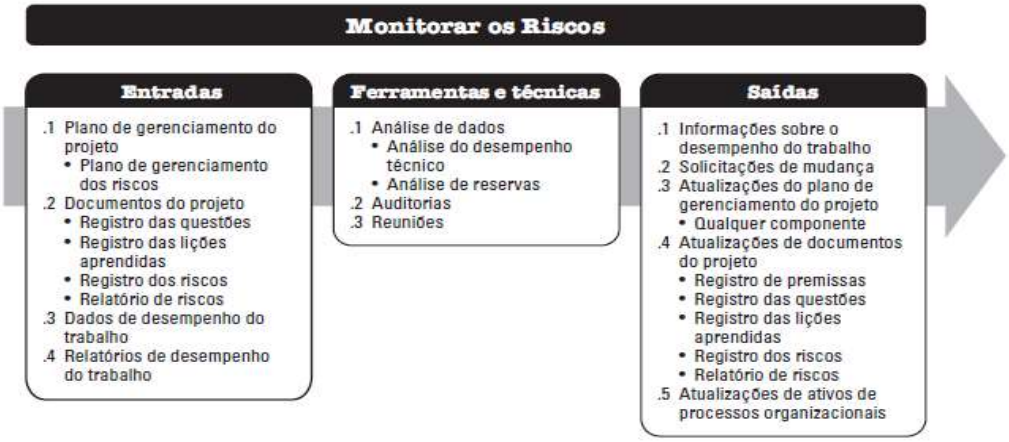
Fonte: PMI (PMBOK, 2013, p. 294)

3.1.3.2 Plano de Gerenciamento de Riscos

Conforme guia PMBOK (PMI, 2013), após gestão e identificação dos riscos, deve-se fazer o monitoramento, registro e relatórios, explicados a seguir.

- Monitoramento dos riscos: processo de acompanhamento dos riscos identificados, identificação e analise dos novos riscos, e avaliação da eficácia do processo de riscos. O principal benefício deste processo e que habilita decisões com base em informações atuais sobre a exposição geral de risco e riscos individuais. A entradas, ferramentas e técnicas e saídas desse processo estão ilustradas na Figura 6.

Figura 6 – Processos de acompanhamento dos riscos



Fonte: PMI (PMBOK, 2013, p. 304)

- Implementar respostas aos riscos: tem como principal benefício deste processo e a garantia de que as respostas acordadas aos riscos sejam executadas conforme planejado à fim de abordar a exposição ao risco geral, minimizar ameaças individuais e maximizar as oportunidades Individuais. As entradas, ferramentas e técnicas e saídas desse processo estão ilustradas na Figura 7.

Figura 7 – Processos de garantia de respostas dos riscos

Fonte: PMI (PMBOK, 2013, p. 640)

- Registrando os riscos: registro dos riscos retém as respostas acordadas aos riscos para cada risco individual e os responsáveis indicados para cada plano de resposta geradas durante o processo Monitorar os Riscos.

- O relatório de risco: o relatório de riscos inclui uma avaliação da atual exposição ao risco geral na medida em que novas informações ficarem disponíveis pelo processo Monitorar os Riscos, assim como a estratégia acordada de resposta aos riscos. Também descreve os principais riscos individuais do projeto com as respectivas respostas planejadas.

4 O ESTUDO DE CASO

4.1 A organização estudada

A empresa de Transporte de Óleo e Gás no segmento de manufatura iniciou suas atividades em 1967, com a fundação de uma pequena empresa familiar, especialista em

serviços de solda e serralheria. No ano de 1987, a empresa passou a fabricar produtos para armazenamento subterrâneo de combustíveis. Já em 2001, a empresa conquistou a Certificação Internacional de Produto (UL), a ISO 9000 e certificação Inmetro. Em 2005, foi inaugurada a unidade de Recife-PB e em 2006, a de Penha-SC, que dois anos depois passou a ser a matriz. Atualmente a empresa tem em seu quadro 780 colaboradores e 100 terceiros envolvidos no processo, sendo que 120 pessoas possuem contato diariamente com sistema ERP. Também possui uma rede de representantes e escritórios no Brasil, Argentina, Paraguai e Uruguai, porém este estudo de caso se restringe à unidade matriz.

4.2 O problema observado

A empresa de produtos para armazenamento, de médio porte, necessita implantar um novo sistema de ERP. O *software* legado atendia basicamente comércio e os controles necessários para o controle de produção foram sendo desenvolvidos especificamente para a empresa. Esse *software* atendeu por um período e a decisão de trocá-lo ocorreu em 2014 e, por isso, foi incluído no planejamento estratégico de 2015 para que a houvesse a substituição. A empresa possuiu um quadro de 780 colaboradores, que estão espalhados em três filiais no Brasil e uma no Paraguai. Com um cenário de incerteza e desconfianças quanto à qualidade da informação do ERP legado, a alta administração fechou o contrato com um ERP de ponta no Brasil.

Sobre isso Escrivão e Veiga (2002, p. 278) colocam que:

> [...] a adoção de um sistema de informação significa mais que uma implantação de tecnologia. Implica em um processo de mudança organizacional, envolvendo não apenas a revisão nos métodos da empresa, mas a prática de uma releitura no contexto cultural da organização.

Com diversos módulos integrados o ERP permeia o gerenciamento da organização de forma confiável, mais para que houvesse a implementação desse projeto o módulo de recursos humanos ficou de fora no primeiro momento, além disso o projeto foi separado em duas fases, sendo que na primeira fase seria utilizada a nova ferramenta em seu formato mais padrão possível, com menor grau de customização possível. Formou-se um comitê gestor de implantação com 30 pessoas (Alta direção, Gestor de TI, Gestores de

áreas especificas e usuários chave) que tinham o objetivo de validar a evolução do projeto e qualquer alteração de escopo, prazo e custos sujeito à aprovação. Para isso foram utilizadas ferramentas e *frameworks* que auxiliassem os gestores de TI na diminuição dos riscos gerado nesse processo.

O Quadro 5 apresenta os riscos levantados, associados ao processo de implantação do novo sistema.

Quadro 5: Riscos identificados no projeto de implantação do novo sistema ERP.

Tipos de riscos	Características
Prazo	Atrasos nas datas de entrega do projeto e na execução das atividades.
Escopo	Aumento no escopo, escopo indefinido, não cumprimento do escopo definido, ausência no gerenciamento de mudanças.
Custo	Aumento do custo em virtude de problemas com estimativas ou improdutividade da equipe, aumento de escopo, trabalho adicional.
Qualidade	Como principais fatores de risco para esta classe estão os problemas relacionados a erros de definição e construção. Ainda como risco em qualidade, temos o não seguimento da metodologia durante os desenvolvimentos, o que poderá acarretar problemas e retrabalhos no momento das inspeções e auditorias da qualidade.

Fonte: Arquivo da empresa (2016).

4.3 Proposta de solução

Para o desenvolvimento de ações utilizou-se a metotologia PMBOK para identificar estratégias possíveis de tratamento dos riscos identificados, de modo a identificar oportunidades e reduzir as ameaças aos objetivos do projeto. As estratégias gerais estão apresentadas no Quadro 6.

Quadro 6: Tipos de riscos e seu tratamento na organização

Riscos	Estratégias
Negativos ou Ameaças	Prevenir, Transferir, Mitigar;
Positivos ou Oportunidades	Explorar, Compartilhar, Melhorar
Ameaças e Oportunidades	Aceitação
Contingências	Transferir, Mitigar

Fonte: PMI (2013).

A partir da classificação dos riscos Quadro 7, os mesmos foram priorizados de acordo com o fator de risco que estes receberam. Itens mais críticos foram os que receberam os fatores mais altos. Tendo os riscos classificados, os mesmos foram analisados de acordo com a melhor estratégia de tratamento para os mesmos. Essas estratégias são detalhadas no Quadro 7.

Quadro 7: Detalhamento do tratamento dos riscos.

Estratégias	Características
Aceitar	A equipe aceita conviver com o risco. Para este caso nenhuma ação é tomada e o risco é apenas acompanhado. No caso de ocorrência do mesmo, deverá ser elaborado um plano de ação para solução do problema gerado pelo risco.
Eliminar	Ocorre uma mudança no escopo do projeto de modo que o risco seja eliminado. Neste caso é elaborado no momento do planejamento um plano de ação para possibilitar a eliminação do risco.
Transferir	Transfere-se a responsabilidade do risco para alguém fora da equipe.
Evitar	Elaboram-se estratégias de modo a tentar diminuir a probabilidade que o risco ocorra. Neste caso é elaborado no momento do planejamento um plano de ação para possibilitar que o risco seja evitado.
Mitigar	Tomada de ações que visam reduzir o risco a patamares aceitáveis.

Fonte: PMI (2013)

Na metodologia do guia PMBOK (PMI, 2013), as reuniões semanais com o time de projeto é uma alternativa utilizada para alinhamento do projeto, na reunião são repassados pontos de dificuldade ou feedback do andamento ao comitê a fim de tomar uma decisão e diminuindo os riscos no projeto de implantação. Com base na análise da situação atual, a estratégia de tratamento do risco podia ser alterada caso necessário, com um plano de ação para o tratamento do mesmo, conforme modelo no Quadro 8.

Quadro 8: Reuniões de Alinhamento da equipe - comitê

Objetivo	Alinhar os trabalhos da equipe para que atuem de maneira integrada durante todo o projeto.
Responsável	Gerente de Projeto.
Pessoas Envolvidas	Analistas de Processos e de Implantação.
Método	Reunião presencial com a equipe de implantação, alinhando pontos críticos, avaliando mudanças necessárias e revisando as pendências do projeto.
Frequência	Semanal.
Convocação	Via *e-mail*.
Duração	Sugestão: 2 horas
Local	Sala do projeto (no cliente) ou no fornecedor.
Observações	Utiliza-se toda a documentação gerada até o momento no intuito de nivelar e compartilhar o conhecimento dos consultores do projeto e também a gerência, apontando as possíveis mudanças de escopo ou riscos identificados.

Fonte: Arquivo da empresa (2016).

A empresa adotou esse procedimento de reuniões semanais registradas em ata com assinatura de todos os envolvidos no processo. Nela, o gerente do projeto repassava para o comitê gestor do projeto os itens relacionados já classificados na tratativa de risco do Quadro 6, tão logo se discutia cada item e pontuava conforme o Quadro 7.

Itens classificados que envolviam modificação no processo original do ERP deveriam ser avaliados e aprovados formalmente em conformidade com o Sistema de Controle de Mudanças para depois serem implantados sem afetar o prazo de implantação do ERP. Pode-se citar como exemplo o item de projeto “Documentação e manual de uso de produtos”, classificado pelo gestor de TI, de acordo com o Quadro 6, como “positivos ou oportunidades”. Sobre esse item o comitê deliberou, conforme Quadro 7, que era necessário mitigar o risco. Por isso foi solicitado para que o manual se tornasse totalmente digital, com opção do cliente baixar (*download)* diretamente pela internet. No comitê acordou-se que essa opção de customização e melhoria seria realizada na segunda fase do projeto, para não atrasar o cronograma. Esse exemplo está sintetizado no Quadro 9.

Quadro 9: Exemplo de classificação e tratamento dos riscos do projeto.

Item do projeto	Acessível	Tipo do risco	Estratégia de tratamento do risco
Documentação e manual de uso do produto	Portal do Cliente, Digital	Positivos ou oportunidades	Mitigar

Fonte: Arquivo da empresa (2016).

A alta direção definiu que na primeira fase de implantação o projeto deveria ser o mais padrão possível, ou seja uso da ferramenta ERP sem customização, para não onerar o projeto e não afetar o cronograma. Ficou evidente que esta definição deve estar de acordo com a cultura e definição da alta direção sobre o grau de risco aceito para o negócio. Estes riscos referiam-se a atrasos nos cronogramas e facilidades existentes no sistema anterior que no sistema atual não seriam contempladas. Tais aspectos representaram um risco ao negócio ou até perda de oportunidade.

4.4 Alinhamento com os frameworks

O alinhamento com os *frameworks* se fez necessário para minimizar os riscos de TI num projeto desse porte e obter o sucesso na implantação. O Quadro 10 foi elaborado com base nos riscos qualitativos apontados pelo comitê gestor. Neste quadro estão listados os itens de projeto e o tipo de risco que representam. Cada item, por sua vez, está associado aos membros da equipe envolvida com aquele item. Esses itens foram discutidos e classificados, para que o projeto ocorresse dentro do prazo.

Quadro 10: Classificação de itens de risco por usuários chave do projeto

Item de risco	Equipe do Projeto	Tipo do risco
Justificativa para o investimento	G2 /G3 /G6 /G7	Oportunidades
Metas e objetivos claros / Cronogramas	G2 /G3 /G4 /G5 /G7 /G6 /G7	Contingências
Suporte do fornecedor / Consultores	G2 /G3/ G5 / G6 / G7	Ameaças
Treinamento do usuário	G3 /G5	Oportunidades
Customização mínima	G2 /G3 /G5 / G6 /G7	Ameaças
Conversão e análise dos dados	G2 /G3 /G4 /G5 /G6	Oportunidades
Suporte da alta gerência	G2 /G5 /G6 /G7	Positivos
Competência / Limitação da equipe do projeto	G2 /G3 /G4 /G5 /G6 /G7	Ameaças
Cooperação interdepartamental	G3 /G4 /G6 /G7	Oportunidades
Comunicação interdepartamental	G2 /G5 /G6 /G7	Positivos
Liderança / Gerenciamento do projeto	G5 /G6 /G7	Positivos
Comitê gestor	G2/ G3	Positivos
Gerenciamento da mudança	G2 /G4 /G5 /G7	Ameaças
Parceria com o fornecedor	G2 /G4 /G5 /G6	Oportunidades
Infraestrutura tecnológica / Arquitetura	G2 /G5 /G6 /G7	Contingências
Sensibilização /Expectativas	G2/ G5 /G6	Oportunidades

Fonte: Arquivo da empresa (2016).

Após identificar os riscos e definir a estratégia de tratamento destes, adotou-se da Norma ISO/IEC 27002, que teve como principal objetivo nortear as regras para implementação e melhoria contínua no quesito de minimizar o impacto de riscos nesse projeto. Determinou-se :

- se respostas ao risco estão sendo implantadas conforme planejado;
- se as ações de respostas ao risco são eficazes conforme o esperado ou se novas respostas devem ser desenvolvidas;
- se as premissas ainda são válidas;
- se a análise da tendência da exposição ao risco tem mudado prioridades;
- se as políticas e procedimentos necessários estão sendo seguidos e adequados para acompanhar os riscos;
- a identificação de novos riscos.

A metodologia Risk IT foi utilizada para colaborar no tramento e monitoramento de alguns riscos identificados. Esse foi o caso, por exemplo, do item "Gerenciamento de mudança", classificado no Quadro 9 como "ameaça". Esse item foi tratado por essa metodologia devido a seu grande impacto, pois o uso da ferramenta padrão do ERP nem sempre atende todos os requisitos da operação da empresa (o que foi o caso nesse estudo). Embora o COBIT estabeleça boas práticas para os meios de gerenciamento de riscos, fornecendo um conjunto de controles para mitigar os riscos de TI no andamento do projeto, o Risk IT define boas práticas, fornecendo uma estrutura para empresas para identificar, administrar e gerenciar riscos de TI, a saber no Quadro 11.

Quadro 11: Técnicas utilizadas na eficácia do monitoramento de risco

Técnicas utilizadas	**Resultados esperados**
Auditores de risco (responsáveis pelo risco) examinam e documentam a eficácia da resposta ao risco.	Plano de ação.
Revisões periódicas dos riscos nas reuniões com o comitê do projeto.	Ações corretivas.
Análise de valor agregado e índices de desempenho.	Solicitações de mudanças no projeto, se necessário e atualização dos planos.
Melhorias desempenho da ferramenta	Atualização de base histórica de projetos base utilização em projetos futuros.

Fonte: ISACA (2011).

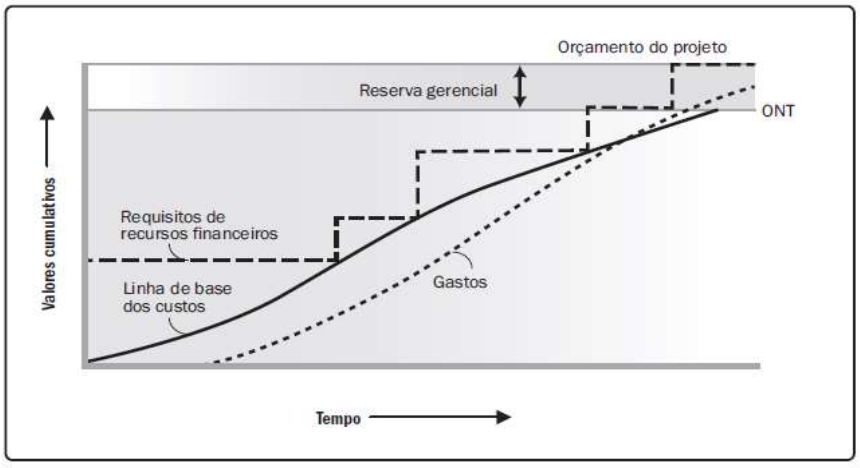
Até esse ponto do projeto, a empresa obteve embasamento na Norma ISO/IEC 27002 e utilizou-se da metodologia PMBOK (2013) para melhorias e acompanhamentos de resultados do projeto. Esses padrões de referência tiveram o COBIT como "guarda chuva" de modo a orientar as o gerenciamento da governança em TI. Também foi utilizado uma análise Qualitativa dos Riscos conforme Quadro 10, apresentado anteriormente. Com esses dados o uso dos *frameworks* Risk IT colaboraram para obter sucesso no gerenciamento de risco e alinhamento com investimento previsto. Dada a extensão desse trabalho, não será relatado em detalhes o uso dos frameworks Risk IT e Val IT.

4.5 Plano de Contingência

Foi necessário no projeto o estabelecimento de um plano de contingência de TI, firmado no escopo inicial do projeto junto com comitê gestor. O plano previa sustentação aos planos de continuidade de negócio. Além disso, algumas ações foram definidas para serem usadas somente se certos eventos ocorressem. Para alguns riscos, o comitê considerou apropriado que o gestor do projeto desenvolvesse um plano de respostas que só seria executado sob determinadas condições predefinidas. Como exemplo pode-se destacar o item "**conversão dos dados",** citado no Quadro 10. Caso fosse necessário implementar o plano de contingências, a conversão seria realizada com os dados dos últimos 5 anos da empresa. Essa ação seria realizada apoiando-se da metodologia do PMBOK (2013), a fim de conseguir manter o cronograma inicial. Dessa forma a base de dados dos outros anos poderia ser convertida posteriormente, após o início de operação do novo sistema, sem atrasar o cronograma definido.

Além disso, estabelecer um determinado nível de contingência de orçamento e de cronograma para riscos emergentes fez-se necessário. As estimativas de duração incluíram reservas de contingência, chamadas de reservas de cronograma, para considerar incertezas no cronograma caso o projeto de implantação do ERP viesse a passar por algum tipo de risco citado no Quadro 5 (Prazo, Custo, Escopo). Esse conceito de reserva contingencial, preconizado pelo PMI (2013), está representado na Figura 8.

Figura 8: Reserva de contingência



Fonte: PMI (2013, p. 264).

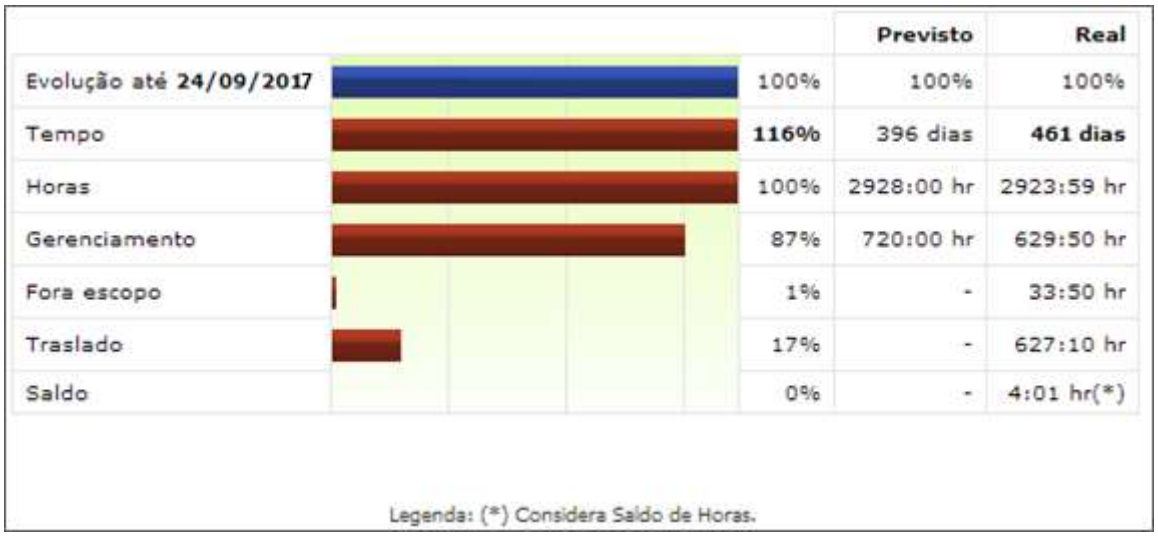
4.4 Desvios da implantação realizada.

Mesmo que a empresa alvo deste estudo esteja atuando há mais de 45 anos no mercado e adote mecanismos de gestão avançados, notou-se que houve desvios no projeto, o que acarretou em atrasos, desgastes e sobrecarga dos funcionários.

Conforme constatado com os colaboradores, a baixa eficácia nos dados importados, a indisponibilidade da equipe, o tempo esgotado para atender o cronograma de virada e o envolvimento dos usuários finais somente na fase final do projeto, gerou resistências à utilização do ERP. Fator esse que contribuiu para a transmissão de conhecimento fosse mais lenta, pois alguns usuários não estavam 100% disponíveis ao projeto, gerando sobrecarga de atividades mais próxima à data de virada do sistema.

Mesmo assim, devido uso das melhores práticas desde o início do projeto, obteve-se ganhos e velocidade para obtenção de um projeto com um pequeno desvio, o que não causou um impacto profundo na implantação do ERP. A Figura 10 apresenta uma visão final do projeto implantado em relação ao tempo, as horas previstas e realizadas, ao gerenciamento, ao escopo e ao traslado.

Figura 10: Indicadores do projeto implantado.



		Previsto	Real
Evolução até **24/09/2017**	100%	100%	100%
Tempo	**116%**	396 dias	**461 dias**
Horas	100%	2928:00 hr	2923:59 hr
Gerenciamento	87%	720:00 hr	629:50 hr
Fora escopo	1%	-	33:50 hr
Traslado	17%	-	627:10 hr
Saldo	0%	-	4:01 hr(*)

Legenda: (*) Considera Saldo de Horas.

Fonte: Dados da empresa, acesso em novembro (2017).

É possível perceber que o tempo estimado excedeu em 65 dias, dos 396 dias projetados, assim como foram utilizadas 292 horas a mais de um total de 2.631 horas previstas. Conclui-se que houve um desvio de 16,41 % do tempo previsto. Sobre isso o Guia PMBOK (2013) destaca que projetos desse porte tendem a variar em média 40% acima do previsto. Tais fatos colaboram para evidenciar que a utilização dos *frameworks* adequados, e que o comprometimento com as metas e objetivos pode trazer consequências positivas para a organização.

6 CONCLUSÕES

Com a realização deste estudo, verificou-se que o uso dos *frameworks* na gestão de TI tem como objetivo promover a previsibilidade e transparência das organizações em seus processos, criando uma forma de monitorar e verificar o processo de gestão, utilizando ferramentas de apoio para diagnósticos mais precisos. Evidenciou-se também que não existe uma receita de bolo sobre quais ferramentas utilizar. Isso dependerá de cada segmento, grau de investimento e impacto fazendo um mix de *frameworks* para melhor aderência, conforme exemplificado no estudo de caso aqui apresentado.

Quanto à ferramenta COBIT para o caso relatado, esta representou um importante recurso para promover o uso das melhores práticas, desde que esteja alinhada com os objetivos do negócio e suas estratégias relacionadas a TI. A sua implementação pode ser de forma gradual, possibilitando para as empresas a criação de bases mais sólidas, atingindo um melhor retorno sobre os investimentos realizados em TI.

Também se pode verificar no estudo de caso que o projeto de implantação do ERP enfrentou desvios. Alguns deles poderiam ser mitigados com o maior envolvimento dos usuários chave ao projeto e o detalhamento mais a fundo de alguns processos que podem necessitar pequenas customizações. Customizações essas que promovem velocidade e segurança do ERP, ou até mesmo trazendo algum valor para o cliente aumentando confiança perante o mercado.

Além disso no estudo de caso o compartilhamento do conhecimento sobre governança, gestão de custos e riscos, a todos os colaboradores envolvidos no projeto representou um ganho para organização, no quesito alinhamento com as melhores

práticas. Além disso, com o uso dessas ferramentas foi possível manter o alinhamento estratégico permitindo a execução do projeto de forma eficiente, eficaz e com gerenciamento de custos empregando esses instrumentos específicos, como solução para cada um desses problemas do projeto de implantação do ERP.

Por fim, destaca-se que outros estudos poderiam ser feitos para estender o presente artigo, detalhando mais o uso das metodologias Risk IT e Val IT, ou realizando uma análise do projeto e seus resultados pela ótica de seus usuários finais.

REFERÊNCIAS

ABNT. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002: Código de Prática para a Gestão da Segurança da Informação**. Rio de Janeiro, 2005.

ABNT. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27005: Gestão de Risco da Segurança da Informação**. Rio de Janeiro, 2008.

AKABANE, Getulio K. **Gestão estratégica da tecnologia da informação: conceitos, metodologias, planejamento e avaliações.** São Paulo. Atlas, 2012.

BECKERS, K.; SCHMIDT, H.; KÜSTER, J. C. & FAßBENDER. S. Pattern-Based **Support for Context Establishment and Asset Identification of the ISO 27000 in the Field of Cloud Computing**. Sixth International Conference on Availability, Reliability and Security, 2011, p.327-333.

DUARTE, M. Y. M. Estudo de caso. In: DUARTE, Jorge; BARROS, Antonio (orgs). **Métodos e técnicas de pesquisa em comunicação**. São Paulo: Atlas, 2006.

IT Governance Institute: Governance of IT Investments, **The Val IT Framework 2.0**. Disponível em: <http://www.isaca.org/Knowledge-Center/Research/Documents/ValIT-Framework2.0-Jul-2008.pdf>.

ESCRIVÃO FIHO, Edmundo; MENDES, Juliana Veiga. **Sistemas integrados de gestão ERP em pequenas empresas**: um confronto entre o referencial teórico e a prática empresarial. Revista Gestão & Produção, São Carlos, v. 9, n. 3, p. 227-296, dez. 2002. Disponível em: < http://www.scielo.br/pdf/gp/v9n3/14570.pdf>. Acesso em: 27/02/2018 de dezembro de 2013.

FERNANDES, Aguinaldo Aragon; ABREU, Vladimir Ferraz de. (2012**) Implantando a Governança de TI: da estratégia à gestão dos processos e serviços**. 3.ed. Rio de Janeiro: Brasport

GIL, A. C. Métodos e técnicas de pesquisa social. 5. ed. São Paulo: Atlas, 1999. _____. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2007.

ISACA. COBIT 5**: Modelo Corporativo para Governança e Gestão de TI da Organização.** Illinois, EUA. 2012.

ISACA (2011). **Risc IT based COBIT**. http://www.isaca.org/Knowledge-Center/Risk-IT-IT-Risk-Management/Pages/Risk-IT1.aspx. Obtido em abril de 2018.

ISO/IEC 27005 (2008) **Information technology -- Security techniques -- Information security risk management** (draft).

LENTO, Luiz Otávio Botelho **Gestão de risco em tecnologia da informação**. Palhoça: Unisul Virtual, 2012.

MARK, Rhodes-Ousley, **Information Security: The Complete Reference**, 2013.

PMI. **Um guia do conhecimento em gerenciamento de projetos. GUIA PMBOK® 5ª ed.** EUA: Project Management Institute, 2013.

ROESCH, Sylvia Maria Azevedo. **Projetos de estágio e de pesquisa em administração**. 3ª. ed. São Paulo: Atlas, 2005.

SCARFONE, K.; GRANCE, T.; MASONE, K. **Computer security incident handling guide special publication 800-61. Revision 1** – National Institute of Standards and Technology, 2008.

STONEBURNER, Gary; GOGUEN, Alice e FERINGA, Alexis. **Risk- Management guide for information technology systems**. Ed.: NIST, 2002. NIST SP 800-30.

VERGARA, S. C. **Métodos de pesquisa em administração**. São Paulo: Atlas, 2005.

VESELY, W. E. *et.al.* **Engineering risk analysis**: technological risk assessment. Hinghan: Martinus Nijhoff Pub., 1984.

VIEIRA, Marconi Fábio. (2007) **Gerenciamento de Projetos da tecnologia da Informação**.2.ed. Rio de Janeiro: Elsevier.

USP. **Guia PMBOK 2013**. Disponível em: <http://www.mediafire.com/file/xojeygypxwgofsm/Guia+PMBOK+6%C2%AA+Edi%C3%A7%C3%A3o.pdf>. Acesso em: 03 março. 2018