

## **GESTÃO DE RISCOS EM TECNOLOGIA DA INFORMAÇÃO: ESTUDO DE CASO NA PERSPECTIVA DA PARTICIPAÇÃO DO USUÁRIO**

**Rosane Machado Maciel**

Professora Mestre do Programa de Graduação da  
Universidade do Vale do Rio dos Sinos- PPGCC/UNISINOS  
Av. Unisinos 950 – São Leopoldo/RS, [machado.rosane@gmail.com](mailto:machado.rosane@gmail.com), (51) 9517-2514

**Adolfo Alberto Vanti**

Professor Doutor do Programa de Pós-Graduação da  
Universidade do Vale do Rio dos Sinos- PPGCC/UNISINOS  
Av. Unisinos 950 – São Leopoldo/RS, [avanti@unisinos.br](mailto:avanti@unisinos.br), (51) 9982-4755

**Maria Cecilia da Silva Brum**

Mestranda do Programa de Pós-Graduação da  
Universidade do Vale do Rio dos Sinos- PPGCC/UNISINOS  
Av. Unisinos 950 – São Leopoldo/RS, [mceciliabrum@hotmail.com](mailto:mceciliabrum@hotmail.com), (51) 9202-1982

**Elson Luciano Weber**

Mestrando do Programa de Pós-Graduação da  
Universidade do Vale do Rio dos Sinos- PPGCC/UNISINOS  
Av. Unisinos 950 – São Leopoldo/RS, [elsonweber@yahoo.com.br](mailto:elsonweber@yahoo.com.br), (51) 9664-0665

### **RESUMO**

Com crescente utilização da tecnologia e dos sistemas de informação, os riscos inerentes à tecnologia da informação necessitam ser gerenciados, a fim de garantir que as práticas decorrentes deste processo não resultem perdas de recursos às organizações. O foco deste trabalho se concentrou em analisar a gestão de riscos em tecnologia da informação (TI) sob a perspectiva da participação do usuário, mediante pesquisa aplicada, uma vez que trata do assunto com vistas à realidade. Quanto à abordagem, trata-se de uma pesquisa qualitativa utilizada em um estudo de caso único. A coleta de dados foi realizada a partir de múltiplas fontes, tais como: entrevistas, questionário e documentos. As entrevistas foram tratadas mediante utilização do software para as análises léxicas. Os resultados decorrentes desta pesquisa indicaram que no caso investigado, apesar de ser identificada uma falta de integração entre a estrutura de gerenciamento de riscos em TI e riscos corporativos, as boas práticas para a GRTI contemplam procedimentos visando satisfazer os requisitos de negócio. Destaca-se que a participação dos usuários nos processos de TI e no gerenciamento do risco de TI, foi identificada, porém esta carece de um maior envolvimento dos usuários no gerenciamento e na efetiva participação no monitoramento dos controles, gerando assim maior consciência da segurança da informação, segundo recomendam em seus estudos: BULGURCU, CAVUSOGLU E BENBASAT (2010) e SPEARS E BARKI (2010).

**Palavras-chave:** Gestão de riscos; Tecnologia da Informação; Usuário; COBIT

## INTRODUÇÃO

Devido a grande parte das transações operacionais se realizarem em ambientes informatizados a tecnologia da informação (TI) vem desempenhando papel cada vez mais importante dentro das organizações (MENDONÇA et al., 2013). A crescente utilização da tecnologia e dos sistemas de informação tornou a TI uma aliada na gestão das organizações. Desta forma, gestão de riscos de TI já não é mais um diferencial em relação à concorrência, e sim, uma vantagem competitiva para as organizações que praticam sua gestão de forma consciente.

Em meio à realidade atual das organizações, uma efetiva gestão de riscos relacionados a TI contribui para transformação de riscos em oportunidades, pois permite a identificação dos fatores responsáveis por perdas em situações imprevistas, como consequência a empresa consegue de um ponto negativo favorecer uma ampliação da sua competitividade. O gerenciamento dos riscos objetiva mitigar acontecimentos indesejados, evitando custos elevados e sem redução das atividades (GERIGK; CORBARI, 2011).

Na gestão dos riscos da tecnologia da informação (TI), o modelo COBIT 4.1 representado pela ISACA (*Information Systems Audit and Control Association*), fornece informações sobre a governança de TI, definindo a estrutura que relaciona os processos de TI, os recursos de TI, e as informações para as estratégias empresariais. O COBIT 4.1 descreve em seu processo PO nº9 (domínio de Planejamento e Organização) maneiras de avaliar e gerenciar os riscos de tecnologia da informação (TI) mesmo que de maneira mais ampla, sugerindo uma estrutura de gerenciamento dos riscos que satisfaça requisitos de negócio como a confidencialidade, a integridade e a disponibilidade. Complementa esta estrutura a necessidade de avaliações periódicas, as recomendações de planos de ação para remediação, e o monitoramento dos riscos (ITGI, 2007).

Dentro deste contexto o problema de pesquisa deste estudo foi definido desta maneira: qual a participação do usuário na gestão de risco da tecnologia da informação (GRTI)? O objetivo geral proposto é de analisar a gestão de riscos em tecnologia da informação (GRTI) sob a perspectiva da participação do usuário.

O artigo está estruturado em cinco seções, incluindo esta introdução, seguido do referencial teórico, da metodologia, do estudo de caso com análise e interpretação dos dados, das considerações finais e, por fim, das referências utilizadas para compor o estudo.

## 2 GESTÃO DE RISCOS EM TECNOLOGIA DA INFORMACAO (GRTI)

A gestão do risco de TI envolve processos, políticas e estruturas que proporcionam conhecer o nível empresarial do risco de TI na empresa. A gestão do risco em TI estrutura e administrada adequadamente pelas corporações, ocasiona a redução de custos ou problemas operacionais relacionados as ameaças inerentes ao ambiente da TI, uma vez que visa a redução destes impactos (WESTERMAN; HUNTER, 2008).

A utilização da TI oferece grandes oportunidades e benefícios para as empresas (ALBERTIN e ALBERTIN, 2012), no entanto, a administração da TI deve estar alinhada a gestão dos negócios e sua governança estar atenta aos riscos percebidos pela GRTI. Isso porque ela é parte integrante da governança corporativa e explora as melhores práticas de TI, focando no apoio à tomada de decisão.

Valor, risco e controle constituem a essência da Governança de TI - GTI (ITGI, 2007). Devido a isso, há uma crescente necessidade da avaliação da gestão dos riscos relacionados a TI, incluindo desde a infraestrutura até os sistemas, pois a GTI necessita ter o completo controle sobre as informações, que são entendidos como elementos-chave de uma boa governança.

Nesse contexto, gerenciar os recursos, as ações e a própria área de TI pode ser uma tarefa complexa, surgindo assim a necessidade da organização de mecanismos que

possibilitem a utilização destes recursos, neste ambiente. Para Simonson, Johnson e Ekstedt (2010) a GTI define de que maneira o uso da tecnologia é gerido e estruturado na organização, e provê mecanismos que permitem o desenvolvimento do planejamento estratégico e planejamento de TI da organização, priorizando o uso da tecnologia. Na busca de assegurar que os princípios da Governança sejam efetivos, as organizações buscam modelos de controle interno e de gestão do risco de TI (FERNANDES; ABREU, 2006).

As organizações precisam investir um alto volume de recursos em TI, sendo estes justificados pela necessidade de se fornecer informações corretas e precisas em tempo adequado, além da necessidade de serem suficientes para garantir que potenciais riscos não afetem o sistema operacional e os controles (COHAN, 2005; LUCHT; HOPPEN; MAÇADA, 2007).

O envolvimento dos usuários nestes investimentos e na identificação da real necessidade destes para geração de bons resultados é fator relevante para a boa gestão da segurança em TI. Para Spears e Barki (2010), no que se refere à gestão em segurança da informação com ênfase nas pessoas, quando existem processos de desenvolvimento ou alteração de sistemas em que os usuários foram envolvidos, os resultados são positivos nas organizações, gerando satisfação e comprometimento.

A participação dos usuários na implementação de projetos relacionados à segurança das informações pode proporcionar um menor risco. Neste contexto, a TI se alinha aos negócios envolvendo-se com os interesses da organização, auxiliando desta forma no alcance das metas globais da companhia. A segurança da informação esta relacionada com a expectativa de todos em que a informação armazenada em um sistema computacional permaneça lá, sem que pessoas não autorizadas possam acessá-las (ALBERTIN e PINOCHET; 2010).

Para Bulgurcu, Cavusoglu e Benbasat (2010), é importante que os gestores compreendam quais fatores motivam os usuários a cumprir as políticas de segurança da informação e, a partir dessa compreensão diagnosticar deficiências para fornecer meios que as minimizem. Para a implantação da segurança da informação é preciso desenvolver planos de segurança, que buscam contemplar os processos de toda a organização.

Os mesmos autores descrevem que os usuários são os principais aliados das organizações nos esforços de reduzir os riscos relacionados à segurança da informação. Neste contexto, a implantação de planos de segurança se faz necessário devido não somente a problemas de natureza dos sistemas, ou dos recursos de TI, mas também quanto a problemas decorridos das atitudes das próprias pessoas que os utilizam, um exemplo que impulsiona o mau uso destes seria a questão dos conflitos de interesses, tratado em teoria específica a teoria da agência (JENSEN; MECKLING, 1976).

Neste contexto, para a redução dos riscos gerados no ambiente de TI mediante a GTI, a literatura pertinente sugere metodologias e conjuntos de melhores práticas, dispostas em *frameworks*, e modelos, dentre eles destaca-se o modelo COBIT 4.1, que foi desenvolvido na década de 90 pela ISACA (*Information System Audit and Control Association*). Este modelo fornece informações sobre a governança de TI definindo a estrutura que liga os processos de TI, os recursos de TI e as informações para as estratégias empresariais.

O COBIT 4.1 é um *framework* modelo de melhores práticas de governança de TI (TUGAS, 2010) constituído de quatro domínios do COBIT 4.1 em sua versão 4.1: 1) planejar e organizar (PO - *Plan and Organise*) – relaciona-se com a maneira como TI contribui para a realização das estratégias do negócio; 2) adquirir e implementar (AI - *Acquire and Implement*) – aborda a pertinência e a possibilidade de fornecimento de soluções que atendem as necessidades do negócio; 3) entrega e suporte (DS- *Deliver and Support*) – preocupa-se com a entrega dos serviços, este processo inclui a prestação de serviços, gestão de segurança e continuidade de apoio aos serviços prestados, gestão de dados e facilidades operacionais; e 4)

monitorar e avaliar (ME- *Monitor and Evaluate*) – este domínio aborda o monitoramento da gestão de TI, acompanhamento mediante controles internos, conformidade regulatória e governança. Por meio destes quatro domínios, nesta mesma versão 4.1 foram identificados trinta e quatro processos de TI nos quais as ligações são realizadas. A visão dos domínios ocorre em três dimensões, a saber: processo de TI, os Recursos de TI, e os requisitos de negócio.

O COBIT 4.1 contempla requisitos de negócios. Dentre eles destacam-se: a) Efetividade: trabalha com as informações relevantes e pertinentes para o processo de negócio bem como a sua entrega de forma correta e em tempo; b) Eficiência: entrega da informação com o melhor uso possível dos recursos; c) Confidencialidade: proteção da informação a fim de que não haja mau uso das mesmas; d) Integridade: fidedignidade, validade da informação de acordo com os valores de negócios e expectativas; e) Disponibilidade: informações disponíveis para o negócio quando requeridas, ligadas à salvaguarda dos recursos necessários e capacidades associadas; f) Conformidade: cumprimento das Leis, contratos e regulamentações; e g) Confiabilidade: entrega de informações apropriadas aos gestores para tomada de decisão, (ITGI, 2007).

O COBIT 4.1 descreve um modelo de maturidade com origem no CMM (*Capability Maturity Model*), sendo que o COBIT 4.1 desenvolveu um roteiro para cada um dos seus 34 processos conforme uma classificação de maturidade. Segundo o ITGI (2007) os níveis de maturidade foram designados como perfis de processos de TI que a organização reconheceria como descrição de possíveis situações atuais e futuras. Melhorar a maturidade reduz riscos e aprimora a eficiência, gerando menor quantidade de erros, processos mais previsíveis e uso eficiente dos recursos sob o ponto de vista de custos (ITGI, 2007).

Para a GRTI o COBIT 4.1 incorpora dentro de seu primeiro domínio (planejar e organizar) o processo P09 - Avaliar e gerenciar os riscos de TI, como um processo que busca criar e manter uma estrutura de gestão de risco, que documenta um nível comum e acordado de riscos de TI. Salienta que qualquer impacto em potencial nos objetivos da empresa causado por um evento não planejado deve ser identificado, analisado e avaliado. Para este processo do COBIT 4.1, os requisitos de negócio, confidencialidade, integridade e disponibilidade foram considerados como primários. Já os de eficácia, eficiência, conformidade e confiabilidade são secundários. Para execução da avaliação e GRTI, objetivos de controle foram detalhados no P09 do COBIT 4.1, estando eles apresentados no Quadro 1:

**Quadro 1: Objetivos de controle - P09 do COBIT 4.1**

OBJETIVO DE CONTROLE	DESCRIÇÃO
Alinhamento da gestão de riscos de TI e de Negócios (PO9.1)	Estabelecer uma estrutura de gestão de riscos de TI alinhada com a estrutura de gestão de riscos da organização (corporação).
Estabelecimento do Contexto de Risco (PO9.2)	Estabelecer o contexto ao qual a estrutura de avaliação de risco é aplicada para assegurar resultados esperados. Isso inclui a definição dos contextos interno e externo de cada avaliação de risco, o objetivo da avaliação e os critérios pelos quais os riscos foram avaliados.
Identificação de Eventos (PO9.3)	Identificar eventos (importante ameaça real que explora significativas vulnerabilidades) com potencial impacto negativo nos objetivos ou nas operações da organização, incluindo aspectos de negócios, regulamentação, aspectos jurídico, tecnologia, parcerias de negócio, recursos humanos e operacionais. Determinar a natureza do impacto e manter esta informação. Registrar e manter um histórico dos riscos relevantes.
Avaliação de Risco (PO9.4)	Avaliar regularmente a probabilidade e o impacto de todos os riscos identificados, utilizando métodos qualitativos e quantitativos. A probabilidade e o impacto associado ao risco inerente e residual devem ser determinados individualmente, por categoria e com base no portfólio da organização.

Resposta ao Risco (PO9.5)	Desenvolver e manter um processo de respostas a riscos para assegurar que controles com uma adequada relação custo-benefício mitiguem a exposição aos riscos de forma contínua. O processo de resposta ao risco deve identificar estratégias de risco, tais como evitar, reduzir, compartilhar ou aceitar o risco, determinar responsabilidades, e considerar os níveis de tolerância definidos.
Manutenção e Monitoramento do Plano de Ação de Risco (PO9.6)	Priorizar e planejar as atividades de controle em todos os níveis da organização para implementar as respostas aos riscos identificadas como necessárias, incluindo a identificação de custos, benefícios e responsabilidade pela execução. Obter aprovações para ações recomendadas aceitação de quaisquer riscos residuais e assegurar que as ações aprovadas sejam assumidas pelos donos dos processos afetados. Monitorar a execução dos planos e reportar qualquer desvio para a Alta Direção.

**Fonte:** Adaptado de ITGI (2007, p.65)

Segundo o ITGI (2007), o gerenciamento do processo de “Avaliar e Gerenciar os Riscos de TI” que satisfaça ao requisito do negócio para a TI de “analisar e comunicar os riscos de TI e seus potenciais impactos nos processos e objetivos de negócio” pode ser realizado de acordo com sua maturidade sendo os graus de maturidade estabelecidos entre 0-Inexistente e 5- Otimizado.

Sugere ainda que estratégias de mitigação de risco devam ser adotadas para minimizar o risco residual a níveis aceitáveis, permitindo que o resultado da avaliação possa ser entendido pelas partes interessadas e expresso em termos financeiros para permitir que elas alinhem o risco a níveis de tolerância aceitáveis (ITGI, 2007).

Para que a organização avalie e gerencie os seus riscos de TI e possa atingir os níveis de maturidade desejáveis é fundamental que todos os objetivos de controle sejam observados, uma vez que, esses possibilitam estabelecer e manter uma estrutura de gestão de risco de TI, bem como, priorizar e planejar atividades de controles em conformidade aos riscos identificados. O adequado gerenciamento dos riscos de TI possibilita que a organização monitore seus riscos em conformidade com as necessidades do negócio. Nesse contexto a participação do usuário torna-se fundamental para que a organização atinja os seus objetivos.

A seção seguinte aborda a metodologia de pesquisa utilizada, apresenta os procedimentos metodológicos adotados neste estudo a fim de que o objetivo desta pesquisa fosse concluído.

### 3 METODOLOGIA

Esta pesquisa objetivou produzir conhecimento sobre a gestão de riscos em tecnologia da informação (GRTI) contemplando a perspectiva da participação do usuário. Neste sentido possui como natureza a de uma pesquisa aplicada, uma vez que trata do assunto com vistas à realidade. Quanto à abordagem, trata-se de uma pesquisa qualitativa utilizada em um estudo de caso único, (SILVA; MENEZES, 2001; GIL, 2009; YIN, 2010).

A opção pela estratégia de pesquisa de estudo de caso único decorreu visando a aquisição de respostas ao problema de pesquisa de forma ampla e aprofundada, já que se trata de uma estratégia de investigação cuidadosa do caso em potencial, capaz de minimizar equívocos e maximizar o acesso necessário à coleta de evidências do estudo de caso, (YIN, 2010).

Como passo metodológico, o estudo contemplou inicialmente a elaboração de um protocolo de estudo de caso. Neste foi incorporado um *framework* metodológico que partiu da categorização dos conceitos estudados na literatura, organizados desta forma para facilitar a construção dos instrumentos de coleta bem como a análise dos dados.

Segundo recomenda Yin (2010), foi encaminhado um pedido de autorização para realização do estudo à empresa objeto da pesquisa. Para seleção da organização a ser estudada, considerou-se: i) A organização possuir o setor de tecnologia da informação (TI), e



comitês ou setores de gestão de riscos. Tais requisitos foram considerados em função da relação da área de TI com os riscos de TI, e do comitê de riscos em função da gestão de riscos corporativos. ii) Interesse e disponibilidade por parte da empresa em participar da pesquisa, fornecendo assim as informações necessárias ao estudo; iii) O acesso à empresa (sede situada no estado do Rio Grande do Sul).

Os procedimentos escolhidos para a coleta dos dados objetivaram a triangulação de métodos para que a geração de evidências fossem suficientes para suportar os achados. Como instrumentos de coleta foram utilizados: documentos, entrevistas e questionários.

## Quadro 2: Detalhamento dos instrumentos de coleta de dados

Instrumento	Objetivo	Seleção / Organização
Documentos	Buscar evidências que pudessem ser cruzadas com as respostas obtidas nas entrevistas e no questionário.	Aqueles que contemplavam os critérios são detalhados: a) Apresentação para o Investidor, (SLC 2012a). b) Código de Ética e Conduta SLC Agrícola, (SLC 2012b); c) Demonstrações Financeiras 2011, (SLC 2012c); d) Fatores de Risco. (SLC, 2012d).
Entrevistas Semi estruturadas	Buscar evidências detalhadas sobre o cotidiano dos entrevistados e sua percepção em relação ao objetivo da pesquisa	O roteiro foi organizado em blocos, e os tópicos de cada bloco foram relacionados as categorias do referencial teórico.
Questionários	Buscar confirmar as evidências geradas nos demais instrumentos mediante avaliação da maturidade do PO9 do Cobit 4.1 e o nível de importância dados aos riscos em TI	O questionário contemplou além de questões fechadas a possibilidade de resposta aberta, pois cada pergunta era seguida da frase: “explique”, buscando entender em profundidade cada nível escolhido (maturidade ou importância) já que o entrevistado tinha a possibilidade de explanar sobre sua opção. Este instrumento foi disponibilizado pessoalmente pelos pesquisadores aos entrevistados.

**Fonte:** Adaptado de Machado (2012, p.56-67)

O tratamento e análise de dados contemplaram a refinação destes e a forma de apresentação das evidências coletadas. Realizou-se a comparação das respostas das entrevistas entre as respostas dos diferentes entrevistados, seguindo a mesma ordenação das categorias consolidadas no Framework metodológico, posteriormente estas análises foram cruzadas com as informações obtidas nos documentos e questionários. Cabe destacar que as entrevistas foram todas gravadas e posteriormente transcritas com o intuito de não haver perda de informações.

Os dados coletados nas entrevistas foram tratados a partir do software *Sphinx Léxica* (versão 5.1), através de um banco de dados composto pelas informações dos participantes. Assim, o *Sphinx Léxica* processou o tratamento da análise de conteúdo de todo o discurso apresentado e fragmentou esse discurso a partir da formulação de categorias de análise (FREITAS e MOSCAROLA, 2002). As combinações da análise de conteúdo e da análise léxica permitiram que os dados das entrevistas fossem analisados.

Para Freitas (2011) os usos destas duas técnicas encobrem diversas das possibilidades que dos dados poderiam surgir, dispondo assim de resultados significativos aplicáveis a uma dada realidade.

Os dados obtidos nas entrevistas foram tratados eliminando qualquer caractere que não fosse letra do corpo do texto. “Foi adicionada antes das perguntas a expressão “P:”, e antes das respostas foi acrescido “R:”. Após este tratamento os dados foram imputados no *software*. A etapa seguinte contemplou a inclusão no sistema das categorias inclusas no *Framework* metodológico, estas foram abreviadas e reduzidas para melhor disposição no mapa fatorial extraído do *software*.

Durante a realização deste estudo, algumas limitações foram observadas. Dentre elas destaca-se a utilização de entrevistas principalmente devido à disponibilidade de tempo dos entrevistados, outro ponto de limitação identificado neste processo são as divergências que podem ocorrer diante da interpretação dos entrevistados e pesquisadores. Contudo, manteve-se o cuidado por parte dos pesquisadores em esclarecer os pontos que pudessem gerar dúvidas no momento das entrevistas e os questionamentos realizados posteriormente para complementar as respostas. Outra limitação identificada refere-se ao uso da estratégia de estudo de caso,

Os procedimentos realizados para coleta, análise e tratamento dos dados permitiram mediante triangulação dos diferentes métodos utilizados, a obtenção dos resultados da pesquisa que foram comparados com a literatura para obtenção das considerações finais.

#### **4 ESTUDO DE CASO – SLC AGRÍCOLA S.A.**

O estudo foi realizado em uma empresa do ramo agrícola cuja matriz localiza-se na cidade de Porto Alegre - RS. Organização fundada em 1977, que têm atividades de agricultura e pecuária, como a produção e comercialização de milho, arroz, feijão soja e algodão, suprimentos para a indústria e revenda de maquinário agrícola. A organização é parte do Grupo SLC que conta com mais empresas dentre elas: SLC Alimentos, Ferramentas Gerais e SLC Comercial.

Atualmente a empresa está organizada na forma de Sociedade Anônima de capital aberto, ou seja, negocia suas ações na bolsa de valores. Em 2011 apurou uma receita operacional maior que trezentos milhões, sendo considerada como empresa de grande porte segundo a carta circular 034 (BNDES, 2012). Seu quadro funcional é composto de 1.985 empregos fixos e 1054 empregos temporários. A capacidade de armazenamento em 2012 é de 470 mil toneladas de grãos e 94 mil toneladas de algodão (SLC, 2012a).

A gestão da empresa está a cargo do seu Diretor Presidente, estando este de forma hierárquica ligado diretamente ao Conselho de Administração que é composto por cinco membros. Subordinados ao Diretor Presidente estão as Diretorias: Financeiras, Novos Negócios, Produção, Recursos Humanos e Vendas. Nas unidades Produtivas (fazendas) a gestão fica a cargo dos Gerentes de fazendas.

O departamento de TI está ligado diretamente à diretoria administrativa financeira e a ele estão ligadas aproximadamente sessenta pessoas. Sua gestão é realizada pelo Gerente Corporativo de TI que tem como principais responsabilidades: gerenciar toda a estrutura de TI (sistemas e infraestrutura) da corporação. Salienta-se a participação do Gerente Corporativo de TI e o Coordenador de sistemas no processo de coleta de dados. Participaram da pesquisa três gestores da empresa, o Gerente Corporativo de TI, o Coordenador de sistemas e o Gerente de RI que também é membro do Comitê de Riscos. Cabe informar que nas próximas seções este participante foi denominado apenas como Membro do Comitê de Riscos. No Quadro 3 as principais características dos respondentes foram descritas.

**Quadro 3:** Principais Características dos Participantes

Aspecto	Gerente Corporativo de TI	Coordenado de Sistemas	Membro do Comitê de Riscos
<b>Principais responsabilidades</b>	Gerenciar a estrutura de TI (sistemas e infraestrutura); Representar a área de TI em reuniões de Diretoria; Gerenciar a atuação dos coordenadores de sistemas e infraestrutura; Gerenciar a parte de telecomunicações do grupo.	Implementação e manutenção de sistemas de todas as fazendas e unidades do grupo; Coordenar a atuação dos analistas de negócio e de empresas terceirizadas (especialistas nos sistemas utilizados pela empresa); Homologação de alterações realizadas pelas terceirizadas e testes de desenvolvimentos internos.	<b>(i) no Comitê</b> – participar das reuniões semanais e mensais; auxiliar nas decisões deliberadas pelo comitê, produzir as informações que apoiaram as decisões do comitê em relação a investidores e mercado mobiliário. <b>(ii) na Gerência de RI<sup>1</sup></b> - Produzir informações trimestrais e anuais para os investidores, e para a CVM <sup>2</sup> . Contato com Investidores e fornecedores.
<b>Tempo na Função e na empresa</b>	Treze anos nesta função, cinco anos na empresa e vinte e quatro anos na área de TI.	Quatro anos nesta função, oito anos na empresa e vinte e três anos na área de TI.	Como Gerente de RI quatro anos, três anos no comitê de riscos, seis anos de empresa.
<b>Formação acadêmica</b>	Graduação em administração de empresa com ênfase em análise de sistemas, e Pós Graduação em análise de sistemas, gestão da produção e governança.	Graduação em administração de empresas com ênfase de análise de sistemas, e Pós Graduação em gestão empresarial.	Bacharel em Administração de empresas e Direito. Não possui Pós Graduação.
<b>Idade</b>	46 anos	46 anos	30 anos

**Fonte:** Adaptado de Machado (2012, p.77)

Dentre os entrevistados observa-se que o Gerente Corporativo de TI é o profissional com maior tempo de experiência. No que concerne à formação acadêmica o membro do Comitê de Riscos é o único profissional sem Pós Graduação, já na faixa etária este participante é o de menor idade, 30 anos.

#### 4.1. Gestão de Riscos em Tecnologia da Informação (GRTI)

O primeiro aspecto a ser destacado é o gerenciamento de TI relacionado ao desenvolvimento do planejamento estratégico, planejamento de TI e gestão de riscos. A percepção do coordenador de sistemas corrobora com a opinião de Simonson, Johnson e Ekstedt (2010), que afirmam que o gerenciamento de TI permite este desenvolvimento. Já o Gerente Corporativo de TI salienta a importância do foco nas necessidades dos usuários.

Possuir uma boa consciência do risco de TI não quer dizer que se está avesso ao risco, mas sim de ter conhecimento dos riscos e tomar decisões em relação a ele. As empresas que adotam a cultura de consciência sobre o risco de TI são mais inteligentes quanto aos riscos que assumirão e a forma que irão os administrar (WESTERMAN; HUNTER, 2008).

A participação de TI no planejamento estratégico foi identificada na resposta do Gerente Corporativo de TI, já o Coordenador de Sistema classifica esta atuação como “pouca”. Isto demonstra que a TI busca trabalhar de forma a colaborar com o planejamento estratégico, porém o envolvimento de todos os colaboradores de TI neste aspecto ainda é fator a ser trabalhado na organização.

<sup>1</sup> RI- Relações com o Investidor.

<sup>2</sup> CVM- Comissão de Valores Mobiliários



No que concerne aos requisitos de negócio (efetividade, eficiência, confidencialidade, integridade, disponibilidade, conformidade e confiabilidade), os gestores destacaram algumas ações/fatores que proporcionam a manutenção destes requisitos na organização. Foram identificadas: i) Investimento no último ano na implantação de um ERP totalmente integrado; ii) Preparação de informações para divulgação a CVM e Investidores; iii) Auditoria externa independente das informações contábeis e dos processos de TI; iv) Implantação da gestão da mudança (modificações solicitadas são pré-aprovadas pelos usuários em um ambiente de teste); v) Atuação da Central de operações NOC (núcleo de operações e controle) que monitora todos os links e acessos; vi) Rotinas de backup das informações.

Cabe destacar dentre as ações, a atuação da auditoria externa nos processos de TI que visa reduzir os riscos inerentes à execução de processos inadequados pela TI, bem como o auxílio no monitoramento das ações relacionadas à manutenção de planos de ações de riscos.

Foram identificadas, adicionalmente em relação às ações para manutenção dos requisitos, algumas vantagens para o caso de estudo, a saber: i) Redução de redigitações ou de reinformação de dados ao longo do processo, evitando a produção de informações errôneas; ii) Melhora da confiança dos investidores nos números produzidos; iii) Melhoria da segurança nos processos após utilização de sistema integrado; iv) Disponibilidade da informação para acionistas de qualquer lugar do país; e v) Garantia da recuperação de informações em caso de possíveis perdas. Tais vantagens possivelmente decorrentes das ações implantadas demonstram a exigência da organização frente ao departamento de TI.

Em relação aos investimentos em TI que podem possibilitar proteger a empresa de riscos, os entrevistados destacaram que estes possibilitam: dados integrados, com muito mais agilidade nos fechamentos; a acurácia na identificar falhas que por ventura podem acontecer; o investimento em torres transmissoras com banco de baterias possibilitou minimizar o risco de indisponibilidade naquele local; a divulgação de informações mais confiáveis.

O investimento em sistema integrado também foi percebido na análise documental das demonstrações financeiras da companhia no ano de 2011. A implementação de um sistema operacional (ERP) foi uma conquista importante naquele ano, porque interligou todas as fazendas com a Matriz de maneira on-line, aprimorando os controles internos da empresa (SLC, 2012).

Pode ser percebido no caso de estudo que a complexidade de uso de alguns recursos tecnológicos impulsiona o custo com treinamento. A companhia poderia neste aspecto atuar de forma mais eficiente e efetiva, buscando uma melhoria nos processos e na cultura dos usuários frente às mudanças tecnológicas, já que isto possibilitaria a redução de riscos gerados no ambiente de TI.

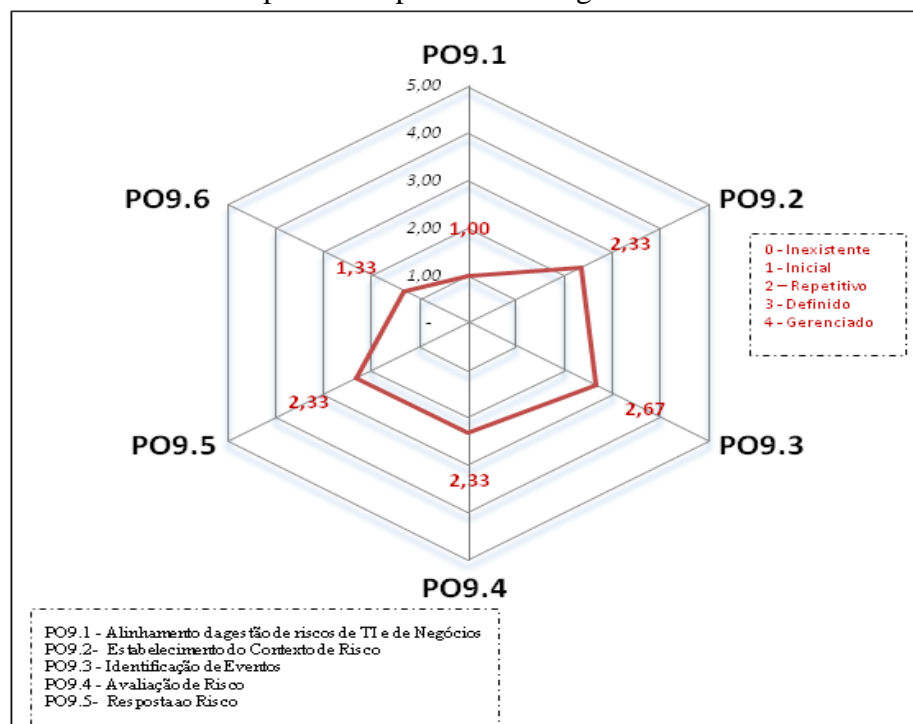
Neste sentido, os entrevistados apontaram alguns riscos associados com o uso da TI, dentre eles destacam-se: i) Vazamento de informações confidenciais (por exemplo, preços e margens de lucro); ii) as fraudes; iii) a invasão de externos aos sistemas provocando instabilidade. Já como ações adotadas para prevenir estes riscos foram identificadas nas entrevistas: i) O controle de acessos externos aos sistemas; ii) Treinamento dos funcionários em relação ao uso da TI; iii) Restrição quanto ao uso do e-mail (correio eletrônico), controle de tamanhos e tipos de arquivos; e iv) a criação de controles e políticas de acesso e uso dos recursos.

Os processos de TI contemplados pelo COBIT 4.1 na gestão de riscos de TI remetem para a adoção de boas práticas para a gestão de riscos de TI. Estas práticas visam garantir de forma primária os requisitos de negócio: confidencialidade, integridade e disponibilidade das informações (ITGI, 2007) bem como, criar estratégias de mitigação para minimizar os riscos a níveis aceitáveis. No que concerne a boas práticas para a GRTI cabe ainda destacar que não foi identificado no caso de estudo uma estrutura de gerenciamento de riscos de TI integrada a estrutura corporativa de gerenciamento de riscos, conforme recomenda o ITGI (2007). Este aspecto se torna negativo, a medida que impede o gerenciamento do risco de TI de estar totalmente integrado aos processos gerenciais externa e internamente.

Quanto aos processos para a gestão de riscos em TI, foi enviado aos respondentes um questionário que contemplou a escolha da adoção de níveis de maturidade para a gestão de riscos em TI, bem como solicitando uma explicação quanto ao motivo da escolha de determinado nível.

A média dos níveis de maturidade do processo de avaliação e gerenciamento dos riscos conforme resposta dos entrevistados é identificada no Gráfico 1. Destaca-se o PO9.3 (identificação de eventos) como o processo com maior nível de maturidade (2,67) e o PO9.1 (alinhamento da gestão de riscos de TI e de Negócios) como o processo com menor nível de maturidade (1,00).

**Gráfico 1:** Maturidade dos processos para avaliar e gerenciar riscos de TI - COBIT 4.1



Fonte: Machado (2012. p.96)

Cabe salientar que a identificação de menor índice de maturidade atribuído ao processo de alinhamento da gestão de riscos de TI e de negócios – PO9.1, está alinhada ao resultado da análise de entrevistas quanto a necessidade da organização trabalhar o nível de envolvimento dos colaboradores de TI no planejamento estratégico.

## 4.2 Participação do usuário na GRTI

Na análise léxica das entrevistas foi identificada a relação de grande significância dos léxicos: segurança, investido (que remete a investimentos em TI), pessoa (usuários),

procedimentos, ERP, estratégia, companhia e mercado. Desta forma, identificam-se variáveis que contemplam o modo que TI é gerenciado no caso de estudo, pode se evidenciar uma preocupação com a participação dos usuários nos procedimentos vinculados ao planejamento estratégico e planejamento de TI.

Contudo, observou-se um distanciamento entre as variáveis: estratégia e pessoa (usuários), fator que comprova a necessidade de um envolvimento mais integrado de todos no entendimento das estratégias de negócio e de TI, afim de uma gestão de riscos mais eficiente. Neste sentido a falta de participação do usuário pode acarretar em menor segurança nas informações, indo ao oposto do que recomendam Spears e Barki (2010).

Pode ser percebido que os entrevistados atuantes na área de TI consideram os investimentos suficientes, estes objetivaram melhorias de sistemas e conectividade como protetores das informações já o membro do Comitê de riscos elencou a necessidade de investimentos em computadores e na comunicação (internet e conexões). Cabe destacar que existe participação dos usuários na validação dos recursos investidos, a qual segue o seguinte fluxo de necessidade de investimentos: 1) Formalização da necessidade pelo usuário; 2) TI identifica o investimento necessário; 3) Solicitação do investimento pelo gestor da área solicitante; 4) O usuário avalia o investimento depois de realizado. Percebe-se que o usuário tem possibilidade de avaliar a qualidade do investimento. Cabe destacar que em investimentos relevantes além da aprovação do gestor, existe a necessidade da avaliação pelo comitê executivo.

A validação pelo usuário dos investimentos corrobora com a visão de Spears e Barki (2010) no que se refere à gestão em segurança da informação com ênfase nas pessoas. Os autores afirmam que quando existem processos de desenvolvimento ou alteração de sistemas em que os usuários foram envolvidos, os resultados têm sido positivos nas organizações, gerando satisfação e comprometimento.

Foi identificado no caso de estudo, riscos e ações associadas ao uso da TI conforme descrito na seção anterior. Neste sentido, a opção da companhia estudada para a criação de controles e políticas para a segurança das informações corrobora com a indicação de Bulgurcu, Cavusoglu e Benbasat (2010) no aspecto da participação dos usuários como aliados da organização nos esforços de reduzir os riscos. A gestão da informação pode ser eficaz quando aborda de forma integrada questões gerenciais e pessoas, no caso de estudo há a necessidade de uma maior sinergia entre estas questões, principalmente no que tange a participação e treinamento dos usuários para utilização da tecnologia.

Colaborando com esta perspectiva a participação dos usuários na adoção de planos de segurança foi citada como importante na percepção dos gestores, que a destacaram como possível, mediante a compreensão por parte dos usuários dos planos de segurança, com comprometimento e ciência das políticas definidas pela corporação. Um exemplo de política adotada pela empresa foi identificado nas palavras do coordenador de sistemas:

[...] Os usuários assinam uma política quando entram na empresa, que se refere a várias questões, como o uso do e-mail (tipo de informação que podem ser enviadas), no uso de má fé nos sistemas, no uso de informações que utilizam no seu dia a dia, enfatizando o cuidado que eles devem ter no uso das informações, tem uma serie de questões que esta política prevê, todos os colaboradores da SLC precisam assinar, estando assim cientes no uso do dia a dia [...].

O mapa fatorial resultado da análise léxica das categorias: segurança nas informações, uso de TI e usuários, contemplou a percepção dos entrevistados sobre tais aspectos. No mapa fatorial se evidenciam as variáveis que permitem a análise entre os léxicos obtidos nas respostas dos entrevistados. A relação de grande significância dos léxicos: pessoa (usuários),

operação, dados, agricultura e integra (integração). Desta forma se evidencia no caso de estudo uma preocupação com a gestão da segurança das informações principalmente na integração dos dados realizados nas fazendas. Estes riscos relacionados ao uso da TI pelos usuários das fazendas foi um fator identificado como ponto de preocupação dos entrevistados, principalmente os riscos decorrentes de problemas de comunicação devido à distância física destes usuários com a área de TI.

Salienta-se a identificação da necessidade de um envolvimento maior dos usuários das fazendas nos processos de TI, a fim de um melhor uso da TI, evitando riscos inerentes a operações realizadas por eles, minimizando desta forma os riscos de TI. Neste sentido, Spears e Barki (2010) recomendam a gestão em segurança da informação com ênfase nas pessoas, pois quando existem processos de desenvolvimento ou alteração de sistemas em que os usuários foram envolvidos, os resultados têm sido positivos nas organizações, gerando satisfação e comprometimento.

De acordo com o COBIT 4.1 (ITGI, 2007), os processos de TI foram gerenciados pelos recursos de TI e respondem aos requisitos de negócio (efetividade, eficiência, confiabilidade, integridade, disponibilidade, conformidade e confiabilidade). Processos mais eficientes podem gerar a uma menor quantidade de erros e o uso eficiente dos recursos. Neste sentido a participação do usuário na homologação destes processos colabora com sua eficiência. No caso de estudo, a homologação dos usuários das solicitações ocorre em um ambiente de teste antes de entrar efetivamente no sistema. Adicionalmente destaca-se neste fluxo a avaliação de usuários chaves em cada setor da empresa que avaliam a necessidade dos demais usuários antes de enviar a solicitação à área de TI.

No fluxo de processo da prestação de serviços de TI pode ser percebida a participação dos usuários, destacando esta participação na homologação dos projetos. Para Spears e Barki (2010) a participação dos usuários na implementação de projetos, testes, análises e monitoramento dos controles garantem menor risco, logo maior segurança.

Em se tratando dos processos de TI, apesar de ser identificada participação do usuário na homologação dos projetos realizados por TI, a participação destes nos processos de negócio vislumbrando o gerenciamento dos riscos de TI ainda carece de ampliação. Esta afirmação pode ser comprovada mediante visualização da relação entre as variáveis: pessoa (que remete a usuários), verifica e evitados (evitar riscos no ambiente de TI) que fora verificados na análise léxica das entrevistas realizada neste estudo.

## **5 CONSIDERAÇÕES FINAIS**

Apesar de ser identificada uma falta de integração entre a estrutura de gerenciamento de riscos em TI e riscos corporativos, pode ser percebido no estudo realizado que as boas práticas para a GRTI contemplam procedimentos com participação dos usuários, havendo uma preocupação com controles sobre acesso, sistemas e a qualidade das informações, visando satisfazer desta forma os requisitos de negócio segundo recomenda o ITGI (2007). Contudo, foi identificado que esta participação ainda precisa ser ampliada para haver uma disseminação de práticas que proporcionem redução efetiva de risco.

Cabe destacar que a participação dos usuários nos processos de TI e no gerenciamento do risco de TI, pode ser identificada, porém esta carece de um maior envolvimento dos usuários no gerenciamento e na efetiva participação no monitoramento dos controles, gerando assim maior consciência da segurança da informação, segundo recomendam em seus estudos BULGURCU, CAVUSOGLU E BENBASAT (2010) e SPEARS E BARKI (2010).

A falta de uma conscientização na empresa deixa os funcionários aptos a cometer erros que poderiam ser facilmente evitados, e tais erros muitas vezes acarretam sérias consequências. Para estimular uma responsabilidade compartilhada em meio à empresa sugere-se a aderência da discussão aberta sobre os riscos inerentes a organização

(WESTERMAN; HUNTER, 2008). Portanto o processo de gestão do risco de TI é a uma forma eficaz para que os gestores com pontos de vista divergentes possam gerar uma visão completa do risco e assim chegar num consenso de como lidar com ele.

Como proposta para estudos futuros se sugere pesquisas focadas na análise da gestão participação do usuário nos controles internos para redução dos riscos em TI em pequenas empresas.

## REFERÊNCIAS

ALBERTIN, A. L.; PINOCHET, L. H. C. Política de segurança de informações: uma visão organizacional para a sua Formulação. Rio de Janeiro: Campus/Elsevier, 2010. 360p.

ALBERTIN, R. M. de M.; ALBERTIN, A. L. Estratégias de governança de tecnologia da informação. São Paulo: Elsevier, 2012.

BANCO NACIONAL DO DESENVOLVIMENTO – BNDES. Carta Circular Nº34. Dispõe sobre: Normas Reguladoras do Produto BNDES Automático. Disponível: <[http://www.bndes.gov.br/SiteBNDES/export/sites/default/bndes\\_pt/Galerias/Arquivos/produtos/download/Circ034\\_11.pdf](http://www.bndes.gov.br/SiteBNDES/export/sites/default/bndes_pt/Galerias/Arquivos/produtos/download/Circ034_11.pdf)> . Acesso em: 20 abr. 2012.

BULGURCU, B.; CAVUSOGLU, H.; BENBASAT, I. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. **MIS Quarterly Executive**, v. 34, n. 3, set. p. 523-548. 2010.

COHAN, P. S. CFOs to Tech: ‘I’ll Spend For The Right Technology’. **Financial Executive**, v.21, n.3, p.30-34, 2005.

FERNANDES, A. A.; ABREU, V. F. de. Implantando a Governança de TI: da estratégia à gestão dos processos e serviços. Rio de Janeiro: Brasport, 2006.

FREITAS, H. Análise de conteúdo: Faça Perguntas as Respostas obtidas com sua ‘Pergunta’! **RAC- Revista de Administração Contemporânea**. Curitiba, v.15, n.4, p.748-760. Jul/ago 2011.

FREITAS, H.; MOSCAROLA, J. Análise de dados quantitativos e qualitativos: casos aplicados usando o Sphinx®. Porto Alegre: Sphinx. 2000.

FREITAS, H.; MOSCAROLA, J. Da observação a decisão: métodos de pesquisa e de análise quantitativa e qualitativa de dados. **RAE- Revista de Administração de Empresas** (Eletrônica), São Paulo, v. 1, n.1, p.1-30. Jan./jun. 2002.

GERIGK, W.; CORBARI, E. C. Risco no ambiente público municipal: um estudo exploratório nos pequenos municípios da região sul do Brasil. **BASE – Revista de Administração e Contabilidade da UNISINOS**. São Leopoldo, v.8, n.1, p.45-57. Jan./mar. 2011.

GIL, A. C.. Como elaborar projetos de pesquisa. 4. ed. São Paulo: Atlas, 2009.

INFORMATION SECURITY GOVERNANCE – ITGI. Cobit 4.1 4.1: objetivos de controle, diretrizes de gerenciamento, modelos de maturidade. 2007. Disponível em:



<<http://www.isaca.org/Knowledge-Center/Cobit 4.1/Documents/Cobit 4.141-portuguese.pdf>>. Acesso em 15 jan. 2011.

JENSEN, M.; MECKLING, W. Theory of the firm: managerial behavior, agency costs and ownership structure. **Journal of Financial Economics**, v.3, p. 305-360, Out. 1976.

LUCHT, R. R.; HOPPEN, N.; MAÇADA, A. C. M..Ampliação do Modelo de Impacto de TI de Torkzadeh e Doll à luz do Processo Decisório e da Segurança da Informação. In:XXXI Encontro ANPAD.**Anais**.p.1-16. Rio de Janeiro,2007.

MACHADO, R. Análise da relação entre a gestão de riscos da tecnologia da informação (TI) e a gestão de riscos corporativos. Dissertação (mestrado em Ciências Contábeis). UNISINOS- Universidade do vale do Rio dos Sinos, São Leopoldo, 2012.

MENDONÇA, C. M. C.; GUERRA, L. C. B.; SOUZA NETO, M. V. de; ARAÚJO, A. G. de Governança de tecnologia da informação: um estudo do processo decisório em organizações públicas e privadas. **RAP - Revista Administração Pública**. Rio de Janeiro, 47(2), p.443-468. Mar./Abr.2013.

SCHNEIDER LOGEMANN & CIA – SLC. Apresentação para o Investidor. Disponível em:<[http://www.mzweb.com.br/SLCAgricola2009/web/conteudo\\_pt.asp?tipo=29143&refbre ad=29097&id=77738&idioma=0&conta=28&submenu=&img=&ano=2011](http://www.mzweb.com.br/SLCAgricola2009/web/conteudo_pt.asp?tipo=29143&refbre ad=29097&id=77738&idioma=0&conta=28&submenu=&img=&ano=2011)> Acesso em 12 abr. 2012a.

\_\_\_\_\_.Código de Ética e Conduta SLC Agrícola. Disponível em: <[http://www.mzweb.com.br/SLCAgricola2009/web/conteudo\\_pt.asp?conta=28&id=77738&tipo=29143&idioma=0](http://www.mzweb.com.br/SLCAgricola2009/web/conteudo_pt.asp?conta=28&id=77738&tipo=29143&idioma=0)> Acesso em 12 abr. 2012b.

\_\_\_\_\_.Demonstrações Financeiras 2011.Disponível em: <[http://www.mzweb.com.br/slcagricola2009/web/arquivos/SLCE3\\_DFP\\_2011\\_PORT.pdf](http://www.mzweb.com.br/slcagricola2009/web/arquivos/SLCE3_DFP_2011_PORT.pdf)> Acesso em 12 abr. 2012c.

\_\_\_\_\_. Fatores de Risco. Disponível em: <<http://www.slcagricola.com.br/>> Acesso em 12 abr. 2012d.

SILVA, E. L. da.; MENEZES, E. M.. Metodologia da pesquisa e elaboração de dissertação. 3°. ed. rev. atual. Florianópolis: Laboratório de Ensino a Distância da UFSC, 2001.

SIMONSON, M. JOHNSON, P. EKSTEDT, M. The Effect of IT Maturity on IT Governance Performance. **Information Systems Management**. Londres: Taylor & Francis Group, LLC , v. 27, p.10-24,. 2010.

SPEARS, J. L.; BARKI, H. User participation in information systems security risk management.**MIS Quarterly Executive**, v.34, n.3, 2010.

TUGAS, F. C. Assessing the level of information technology (IT) processes performance and capability maturity in the Philippine food, beverage, and tobacco (fbt) industry using the Cobit 4.1 framework 2010. **Academy of Information and Management Sciences Journal**. v.13, n.1. 2010.

WESTERMAN, G.; HUNTER, R.. O risco de TI: convertendo ameaças aos negócios em vantagem competitiva. São Paulo: M. Books do Brasil, 2008.

YIN, R. K. Estudo de Caso: Planejamento e métodos. 4 ed. Porto Alegre: Bookman, 2010. 248 p.